清华大学计算机系列教材

图论与代数结构

戴一奇 胡冠章 陈卫

TSINGHUA COMPUTER
TSINGHUA COMPUTER
TSINGHUA COMPUTER
TSINGHUA COMPUTER
TSINGHUA COMPUTER
TSINGHUA COMPUTER
TSINGHUA COMPUTER
TSINGHUA COMPUTER
TSINGHUA COMPUTER
TSINGHUA COMPUTER
TSINGHUA COMPUTER
TSINGHUA COMPUTER

清华大学出版社

图论与代数结构

戴一奇　胡冠章　陈　卫

清华大学出版社

（京）新登字 158 号

内 容 简 介

离散数学是计算机专业的主要数学基础，本书与“数理逻辑与集合论”一起构成了清华大学计算机系的离散数学教材，全书共分 10 章：图论的基本概念；道路与回路；树；平面图与图的着色；匹配与网络流；图的连通性；代数结构预备知识；群；环和域；格与布尔代数。

全书结构紧凑、内容精炼、证明严谨、语言流畅。为了便于读者理解和掌握基本理论，书中提供了丰富的例题，同时给出了众多良好的图算法，并进行了复杂性分析。此外，每章附有较多习题，其难度恰当。

本书可作为计算机专业学生的教科书或参考书，也可供计算机工程技术人员作为参考。

图书在版编目（CIP）数据

图论与代数结构/戴一奇等编著。—北京：清华大学出版社，1995
ISBN 7-302-01814-6

Ⅰ. 图… Ⅱ. 戴… Ⅲ. ①图论②代数-结构（数字） Ⅳ. ①O157.5②O15

中国版本图书馆 CIP 数据核字（95）第 03642 号

出版者：清华大学出版社（北京清华大学学研大厦，邮编 100084）
http://www.tup.tsinghua.edu.cn
印刷者：北京通州宏飞印刷厂
发行者：新华书店总店北京发行所
开　本：787×1092 1/16　**印张**：14.25　**字数**：335 千字
版　次：1995 年 8 月第 1 版　2002 年 5 月第 5 次印刷
书　号：ISBN 7-302-01814-6/TP・810
印　数：9001～11000
定　价：12.90 元

前　言

离散数学是计算机专业的基础数学课程，它以离散量为研究对象，主要包括数理逻辑、集合论、图论和代数结构四部分内容。

清华大学计算机科学与技术系把离散数学安排为“数理逻辑与集合论”，“图论与代数结构”两门课程，分两个学期讲授，各占50学时。

本书分两大部分，其中一～六章是图论，在第一章介绍了图的基本概念及其代数表示方法，第二至第六章分别详细讨论了道路与回路、树、平面图与图的着色、匹配与网络流、图的连通性等图论的主要内容，并且将它们与计算机的应用紧密结合，分析介绍了众多良好的图算法，给出其正确性证明与复杂度分析，这样，使读者在图的应用及算法的设计与分析方面能得到较好的训练与培养。第七～十章是代数结构部分，主要讨论了群、环和域、格与布尔代数等内容，它们都是抽象代数的基本内容，是计算机科学的重要数学基础。

书中给出了大量的例题，它们不但有助于对概念的理解，同时也帮助读者掌握不同的证明方法。各章后面附有较多的习题，有难有易，同时还有一定数量的上机题，可以帮助读者熟悉掌握图的编程技巧。

本书是作者在使用多年“图论与代数结构”讲义的基础上完成的。其中戴一奇修改了第一～六章，胡冠章修改第七～九章，并审定了全书，陈卫修改了第十章。在出版过程中，得到了周远清教授和林行良教授的热情支持，贾志红同志完成了全部书稿的输入与排版，在此一并表示感谢。

由于水平所限，本书难免出现错误与缺点，恳切希望得到广大读者，特别是讲授此课程教师们的批评与指正。

目　　录

第一章　基本概念 ……………………………………………… (1)

1.1　图的概念……………………………………………… (1)

1.2　图的代数表示……………………………………………… (5)

习题一 ……………………………………………… (9)

第二章　道路与回路 ……………………………………………… (11)

2.1　道路与回路……………………………………………… (11)

2.2　道路与回路的判定……………………………………………… (13)

2.3　欧拉道路与回路……………………………………………… (16)

2.4　哈密顿道路与回路……………………………………………… (18)

2.5　旅行商问题……………………………………………… (21)

2.6　最短路径……………………………………………… (24)

2.7　关键路径……………………………………………… (28)

2.8　中国邮路……………………………………………… (32)

习题二 ……………………………………………… (35)

第三章　树 ……………………………………………… (38)

3.1　树的有关定义……………………………………………… (38)

3.2　基本关联矩阵及其性质……………………………………………… (39)

3.3　支撑树的计数……………………………………………… (41)

3.4　回路矩阵与割集矩阵……………………………………………… (46)

3.5　支撑树的生成……………………………………………… (52)

3.6　Huffman 树 ……………………………………………… (56)

3.7　最短树……………………………………………… (59)

3.8　最大分枝……………………………………………… (62)

习题三 ……………………………………………… (66)

第四章　平面图与图的着色 ……………………………………………… (69)

4.1　平面图……………………………………………… (69)

4.2　极大平面图……………………………………………… (70)

4.3　非平面图……………………………………………… (72)

4.4　图的平面性检测……………………………………………… (73)

4.5　对偶图……………………………………………… (79)

4.6　色数与色数多项式……………………………………………………（ 83 ）
习题四 ……………………………………………………………………（ 87 ）

第五章　匹配与网络流 ……………………………………………………（ 89 ）
5.1　二分图的最大匹配……………………………………………………（ 89 ）
5.2　完全匹配………………………………………………………………（ 91 ）
5.3　最佳匹配及其算法……………………………………………………（ 94 ）
5.4　最大基数匹配…………………………………………………………（ 99 ）
5.5　网络流图………………………………………………………………（104）
5.6　Ford-Fulkerson 最大流标号算法……………………………………（107）
5.7　最大流的 Edmonds-Karp 算法………………………………………（109）
5.8　最小费用流……………………………………………………………（111）
习题五 ……………………………………………………………………（114）

第六章　图的连通性 ………………………………………………………（116）
6.1　割点、割边和块 ………………………………………………………（116）
6.2　结点与边的连通度……………………………………………………（118）
6.3　明格尔定理……………………………………………………………（122）
6.4　连通度的判定…………………………………………………………（123）
6.5　无向图的 DFS 算法与图的块划分 …………………………………（126）
6.6　有向图的 DFS 算法与强连通块划分 ………………………………（129）
习题六 ……………………………………………………………………（133）

第七章　代数结构预备知识 ………………………………………………（135）
7.1　集合与映射……………………………………………………………（135）
7.2　等价关系………………………………………………………………（138）
7.3　代数系统的概念………………………………………………………（140）
7.4　同构与同态……………………………………………………………（143）
习题七 ……………………………………………………………………（146）

第八章　群 …………………………………………………………………（148）
8.1　半群……………………………………………………………………（148）
8.2　群、群的基本性质 ……………………………………………………（152）
8.3　循环群　群的同构……………………………………………………（156）
8.4　变换群和置换群　Caylay 定理 ………………………………………（161）
8.5　陪集和群的陪集分解　Lagrange 定理 ………………………………（165）
8.6　正规子群与商群………………………………………………………（169）
8.7　群的同态、同态基本定理 ……………………………………………（171）

8.8 群的直积 …… (176)
习题八 …… (177)

第九章 环和域 …… (180)
9.1 环及其性质 …… (180)
9.2 理想、商环 …… (185)
9.3 环的同态 …… (187)
9.4 域的概念 …… (191)
习题九 …… (193)

第十章 格与布尔代数 …… (196)
10.1 格及其基本性质 …… (196)
10.2 子格、同态与同构 …… (202)
10.3 分配格与有补格 …… (206)
10.4 布尔代数 …… (211)
10.5 布尔表达式 …… (216)
习题十 …… (218)

第一章　基本概念

1.1　图的概念

世界上许多事物以及它们之间的联系都可以用图形直观地表示。这时人们往往用结点表示事物，用边表示它们之间的联系。这种由结点和边构成的图形就是图论所研究的对象。

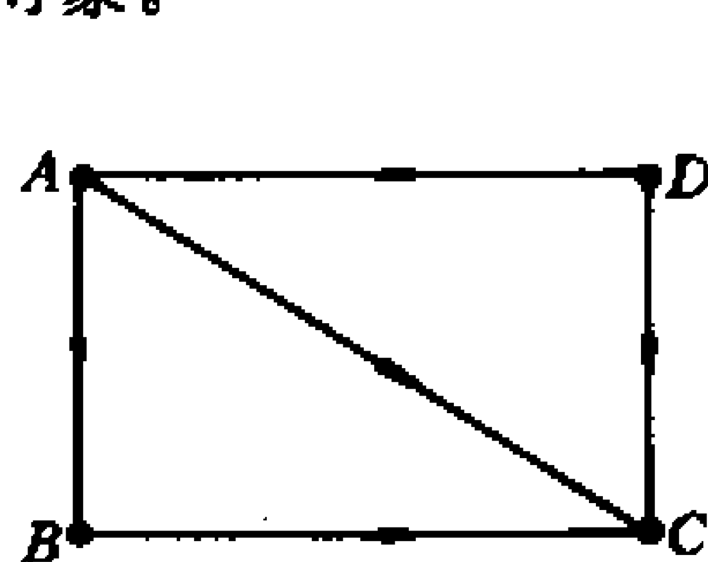
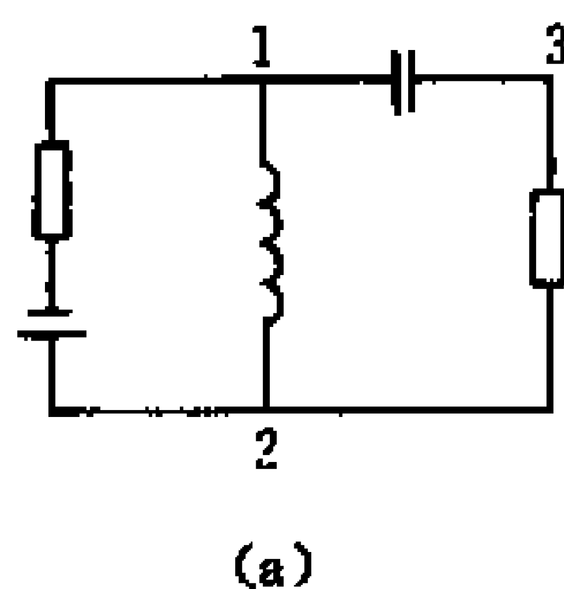
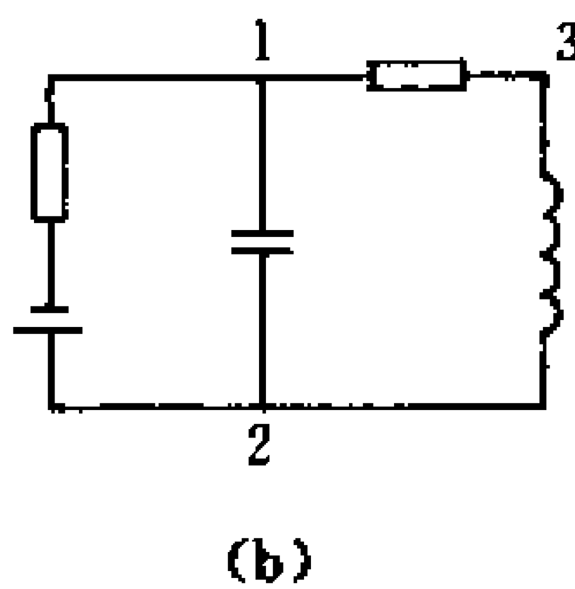


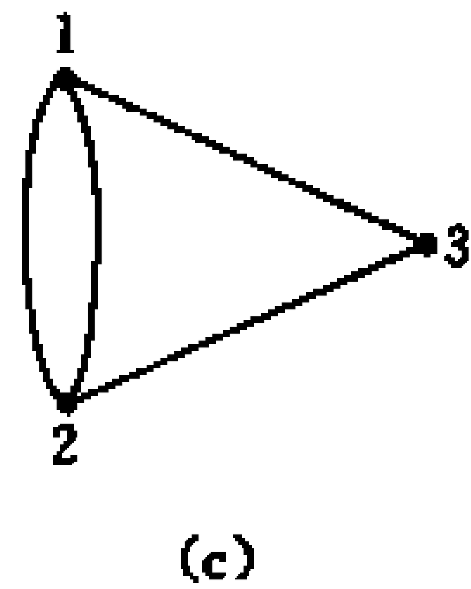
图　1.1



(a)



(b)



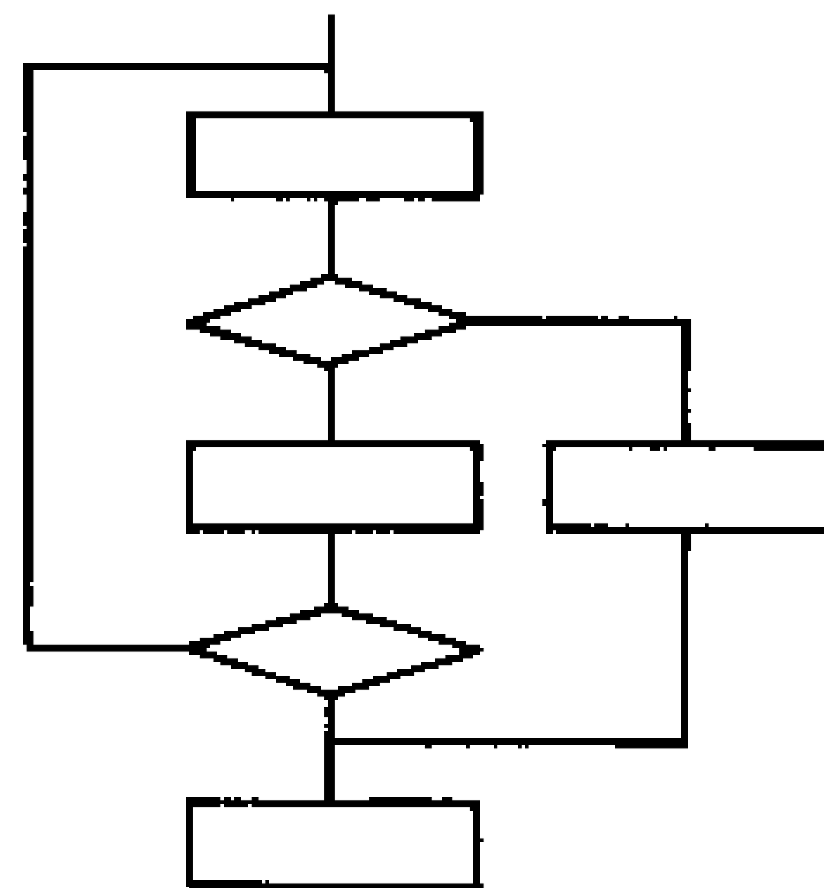
(c)

图　1.2

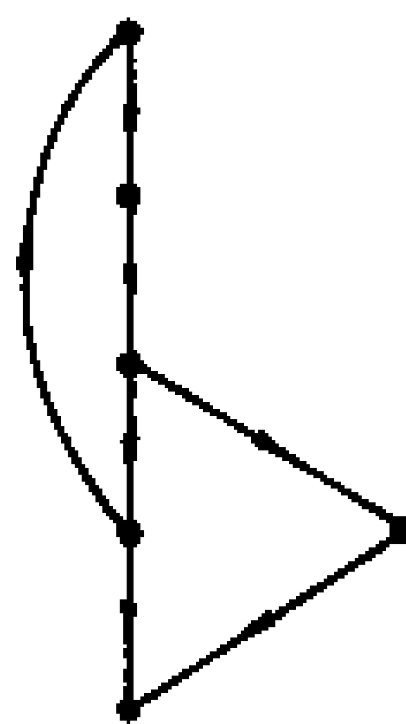
例 1.1.1　A、B、C、D 4 个队进行循环赛。为了解当前各队的胜负情况，可以用结点表示队，用有向边(u,v)表示 u 队胜 v 队。例如图 1.1 表示 A 胜 B、C、D；B 胜 C；D 胜 C，而 B 和 D 之间还没有比赛。

例 1.1.2　两个直流电路如图 1.2(a)(b)。基尔霍夫定律指出：电路特性只与电路网络的拓扑性质有关，而与支路元件的特性无关。因此都可以将它们转化为图 1.2(c)进行研究。

例 1.1.3　人们常用框图的形式来帮助编写或描述程序。当需要对程序进行分析时，也往往用结点表示程序框，用有向边表示它们之间的顺序关系，如图 1.3 。



(a)



(b)

图　1.3

定义 1.1.1　二元组$(V(G),E(G))$称为图。其中 $V(G)$是非空集合，称为结点集，$E(G)$是 $V(G)$诸结点之间边的集合。常用 $G=(V,E)$表示图。

图可以分为有限图与无限图两类。本书只讨论有限图，即 V 和 E 都是有限集。给定某个图 $G=(V,E)$，如果不加特殊说明，就认为 $V=\{v_1,v_2,\cdots,v_n\}$，$E=\{e_1,e_2,\cdots,e_m\}$，即结点数$|v|=n$，边数$|E|=m$。

图 G 的边可以是有方向的，也可以是无方向的。它们分称为有向边(或弧)和无向边，用 $e_k=(v_i,v_j)$表之。这时我们说 v_i 与 v_j 是相邻结点；e_k 分别与 v_i，v_j 相关联。如果 e_k 是有

向边，称 v_i 是 e_k 的始点，v_j 是 e_k 的终点；并称 v_i 是 v_j 的直接前趋，v_j 是 v_i 的直接后继。如果 e_k 是无向边，则称 v_i，v_j 是 e_k 的两个端点。全部由有向边构成的图叫有向图；只由无向边组成的图叫无向图；既有有向边又有无向边构成的图称为混合图。例如图 1.4(a)是有向图，(b)是无向图，(c)是混合图。在图 G 中，只与一个结点相关联的边称为自环，在同一对结点之间可以存在多条边，称之为重边。含有重边的图叫多重图。比如图 1.4(a)(b)中 a_4，e_4 分别是自环，a_1，a_2 和 e_1，e_2，e_3 分别是重边。

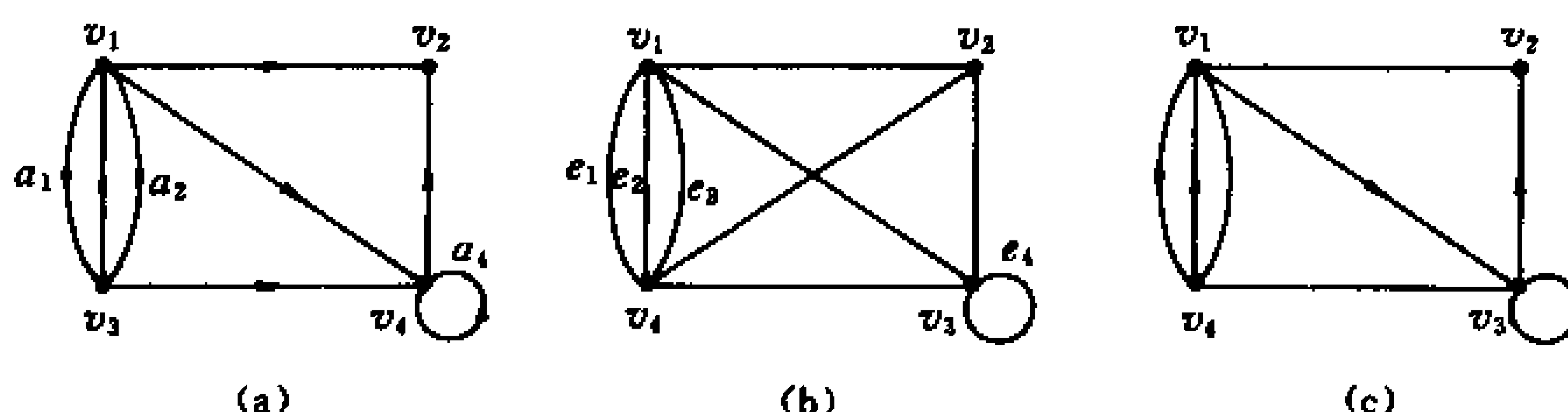


图 1.4

定义 1.1.2 $G=(V,E)$的某结点 v 所关联的边数称为该结点的度，用 $d(v)$表示。如果 v 带有自环，则自环对 $d(v)$的贡献为 2。

例如图 1.4(a)中，$d(v_1)=5$，$d(v_2)=2$，$d(v_3)=5$，$d(v_4)=4$。(b)中，$d(v_1)=5$，$d(v_2)=3$，$d(v_3)=5$，$d(v_4)=5$。有向图中由于各边都是有向边，因此每个结点 v 还有其正度($d^+(v)$)和负度($d^-(v)$)。$d^+(v)$的值是以 v 为始点的边的数目，$d^-(v)$是以 v 为终点的边的数目。显然有 $d^+(v)+d^-(v)=d(v)$。

定义 1.1.3 任意两结点间最多只有一条边，且不存在自环的无向图称为简单图。

以下所说的图在不加说明的情况下指的是无向图。

没有任何边的简单图叫空图，用 N_n 表示；任何两结点间都有边的简单图称为完全图，用 K_n 表示。K_n 中每个结点的度都是 $n-1$。

图 G 具有以下基本性质。

性质 1.1.1 设 $G=(V,E)$有 n 个结点，m 条边，则

$$\sum_{v\in V(G)} d(v) = 2m。$$

证明：由于每条边 $e=(u,v)$对结点 u 和 v 度的贡献各为 1，因此 m 条边对全部结点度的总贡献就是 $2m$。

性质 1.1.2 G 中度为奇数的结点必为偶数个。

证明：G 中任一结点的度或为偶数或为奇数，设 V_e 是度为偶的结点集，V_o 是度为奇的结点集。于是有

$$\sum_{v\in V_e} d(v) + \sum_{v\in V_o} d(v) = 2m，$$

因此 $\sum_{v\in V_o} d(v)$ 为偶数，即 V_o 中含有偶数个结点。

性质 1.1.3 有向图 G 中正度之和等于负度之和。

这是因为每条边对结点的正、负度贡献各为 1。

性质 1.1.4　K_n 的边数是 $\frac{1}{2}n(n-1)$。

证明：K_n 中各结点的度都是 $(n-1)$，由性质 1.1.1 即得。

性质 1.1.5　非空简单图 G 中一定存在度相同的结点。

证明：设 G 中不存在孤立结点，则对 n 个结点的简单图，每个结点度 $d(v)$ 的取值范围是 $1\sim(n-1)$，由抽屉原理，一定存在两个度相同的结点。若存在孤立结点，亦类似可证。

定义 1.1.4　如果图 $G=(V,E)$ 的每条边 $e_k=(v_i,v_j)$ 都赋以一个实数 w_k 作为该边的权，则称 G 是赋权图。特别地，如果这些权都是正实数，就称 G 是正权图。

图 1.5 就是一个正权图。权可以表示该边的长度，时间，费用或容量等。

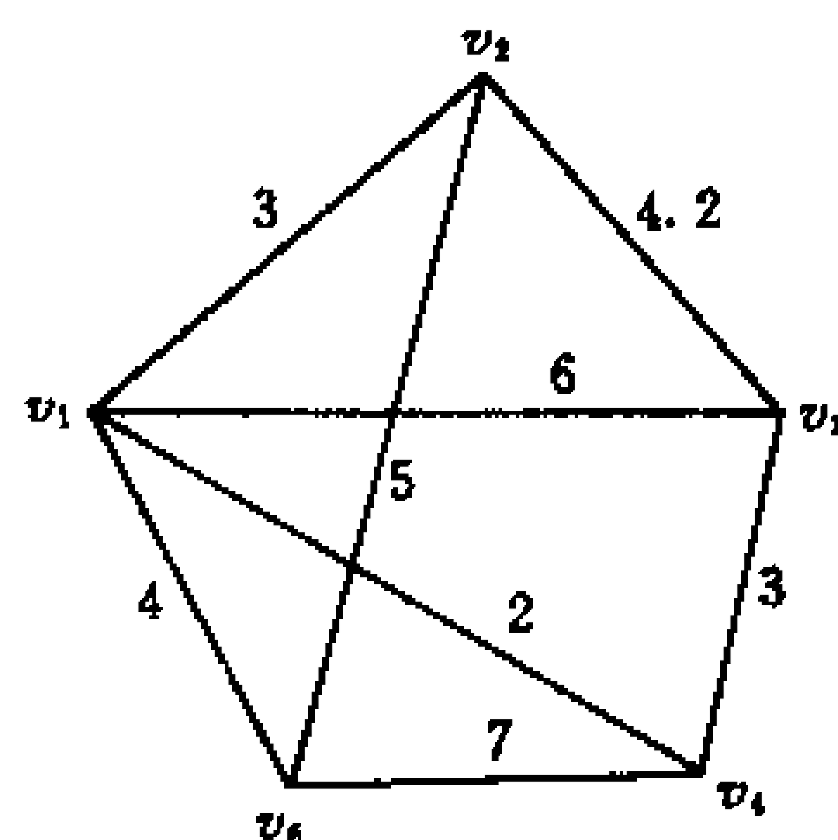


图 1.5

定义 1.1.5　给定 $G=(V,E)$，如果存在另一个图 $G'=(V',E')$，满足 $V'\subseteq V$，$E'\subseteq E$，则称 G' 是 G 的一个子图。特别地，如果 $V'=V$，就称 G' 是 G 的支撑子图或生成子图；如果 $V'\subseteq V$，且 E' 包含了 G 在结点子集 V' 之间的所有边，则称 G' 是 G 的导出子图。

例如，图 1.6 中的 G_1 和 G_2 分别是 G 的支撑子图和导出子图，G_3 是 G 的子图。按照子图的定义，显然 G 也是它自身的子图，而且既是支撑子图，也是导出子图。空图也是 G 的子图，而且是支撑子图。它们都称为平凡子图。

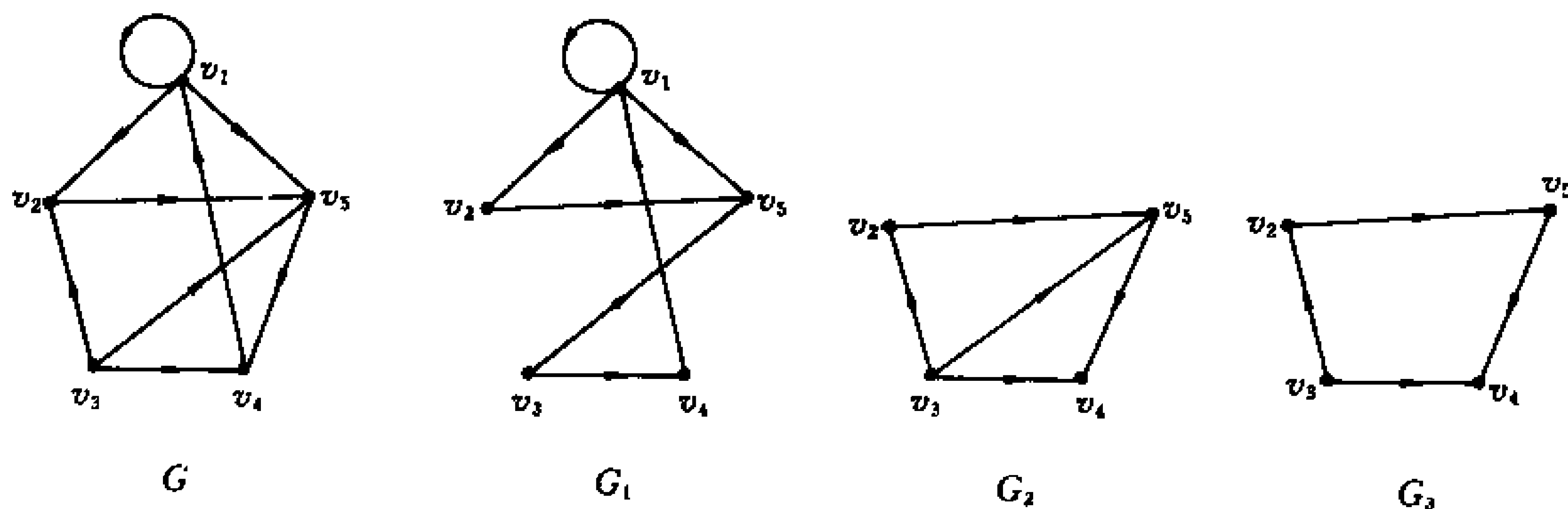


图 1.6

定义 1.1.6　给定两个图 $G_1=(V_1,E_1)$，$G_2=(V_2,E_2)$。令 $G_1\cup G_2=(V,E)$，其中 $V=V_1\cup V_2$，$E=E_1\cup E_2$，$G_1\cap G_2=(V,E)$，其中 $V=V_1\cap V_2$，$E=E_1\cap E_2$，$G_1\oplus G_2=(V,E)$，其中 $V=V_1\cup V_2$，$E=E_1\oplus E_2$，分别称为 G_1 和 G_2 的并、交和对称差。

例如图 1.7 中 G_1 和 G_2 的并、交、对称差分别是(a)、(b)和(c)。

在 G 中删去一个子图 H，指删掉 H 中的各条边，记作 $G-H$，特别地，对于简单图 G，称 K_n-G 为 G 的补图，记作 $\overline{G}$。例如图 1.7 中 G_1 的补图是(d)。从 G 中删去某个结点 v 及其关联的边所得到的图记作 $G-v$。从 G 中删去某条特定的边 $e=(u,v)$，记作 $G-e$。例如图 1.6 中 $G-v_1=G_2$，$G_2-(v_3,v_5)=G_3$。显见 $G-v$ 是 G 的导出子图，而 $G-e$ 是 G 的支撑子图。如果在 G 中增加某条边 e_{ij}，可记作 $G+e_{ij}$，例如 $G_3+(v_3,v_5)=G_2$。

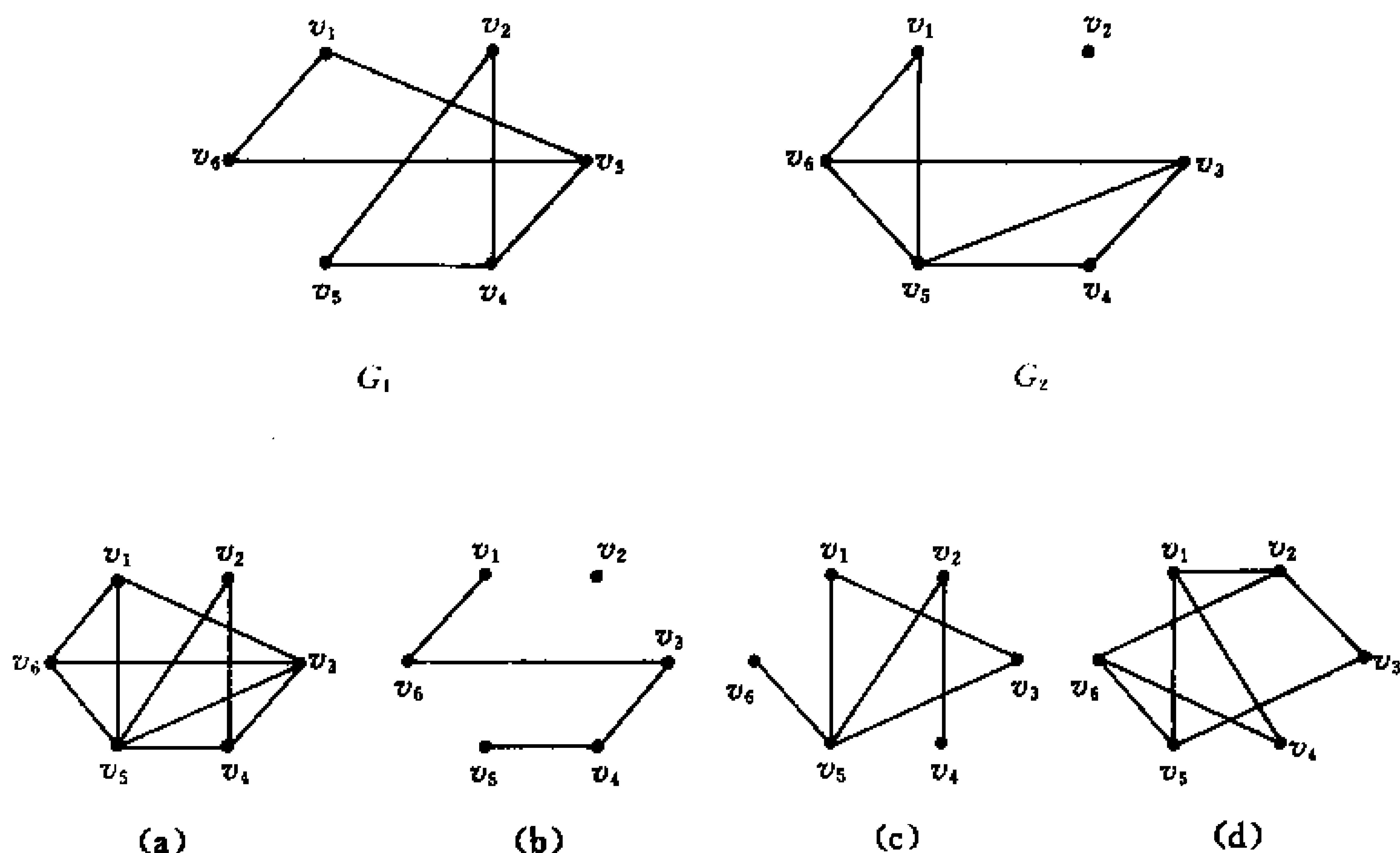


图 1.7

如果 G 是无向图,则 $\Gamma(v)=\{u\mid(v,u)\in E\}$ 称为 v 的邻点集。

定义 1.1.7 设 v 是有向图 G 的一个结点,则

$$\Gamma^{+}(v)=\{u\mid(v,u)\in E\}$$

称为 v 的直接后继集亦称外邻集;相应地

$$\Gamma^{-}(v)=\{u\mid(u,v)\in E\}$$

称为 v 的直接前趋集亦称内邻集。

例如图 1.6(a)的 $\Gamma^{+}(v_1)=\{v_1,v_2,v_5\}$, $\Gamma^{+}(v_2)=\{v_5\}$; $\Gamma^{-}(v_1)=\{v_1,v_4\}$, $\Gamma^{-}(v_2)=\{v_1,v_3\}$。图 1.5 中, $\Gamma(v_1)=\{v_2,v_3,v_4,v_5\}$, $\Gamma(v_2)=\{v_1,v_3,v_5\}$。

给定了结点数目及它们之间的相邻关系,便很容易画出图 G,不过它的形状不是唯一的。这种形状不同但结构相同的图叫做同构。

定义 1.1.8 两个图 $G_1=(V_1,E_1)$, $G_2=(V_2,E_2)$,如果 V_1 和 V_2 之间存在双射 f,而且 $(u,v)\in E_1$,当且仅当 $(f(u),f(v))\in E_2$ 时,称 G_1 和 G_2 同构。记作 $G_1\cong G_2$。

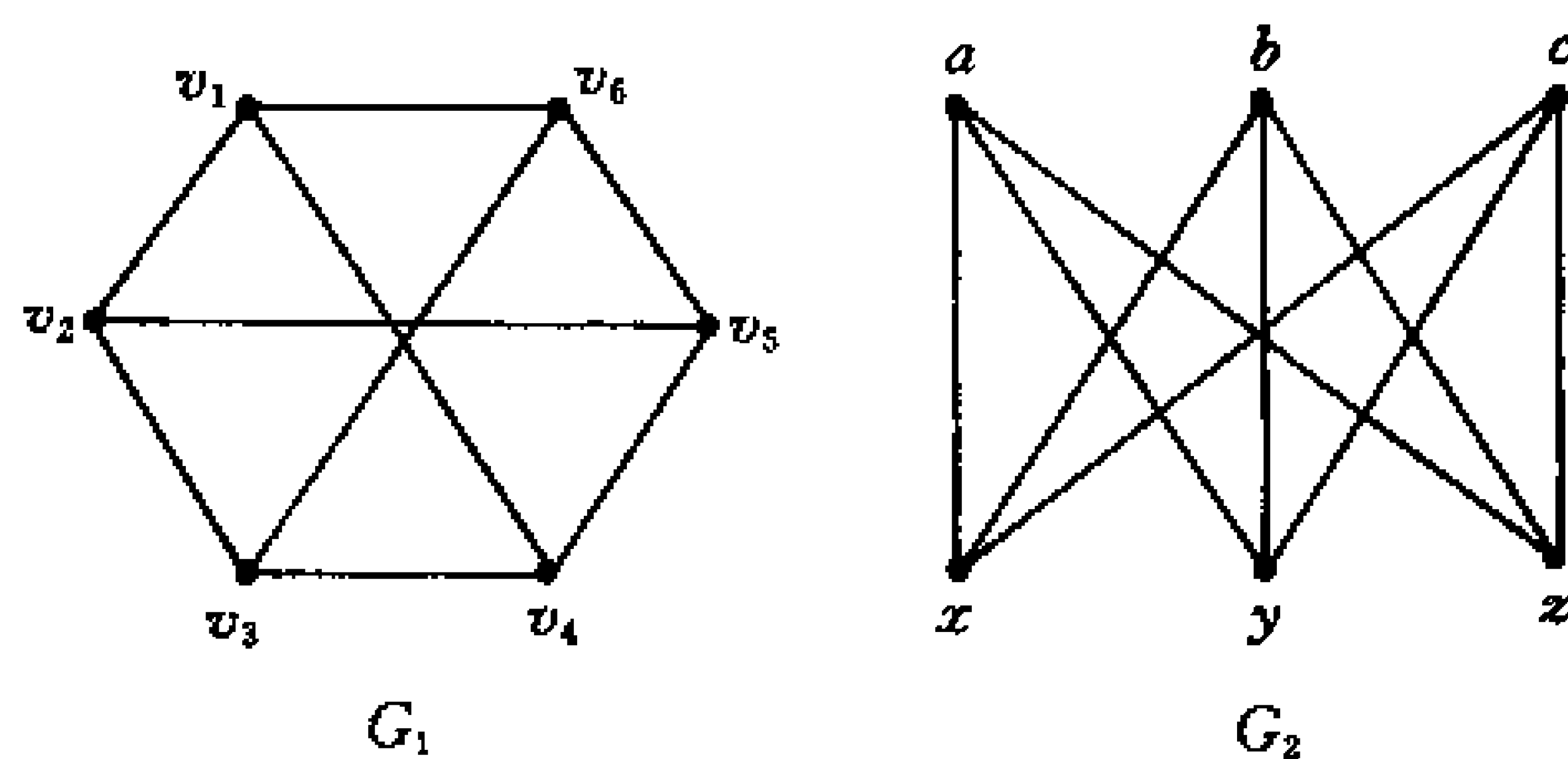


图 1.8

例 1.1.4 图 1.8 的 G_1 和 G_2 是同构的。因为设 $f(v_1)=a$, $f(v_2)=x$, $f(v_3)=b$, $f(v_4)=y$, $f(v_5)=c$, $f(v_6)=z$ 时,对任意 $e=(u,v)\in E_1$,都有 $e'=(f(u),f(v))\in E_2$,反之亦然,即

$(v_1,v_2)\in E_1\leftrightarrow(f(v_1),\quad f(v_2))=(a,x)\in E_2$,

$(v_1,v_4)\in E_1\leftrightarrow(f(v_1),\quad f(v_2))=(a,y)\in E_2$,

$(v_1,v_6)\in E_1\leftrightarrow(f(v_1),\quad f(v_2))=(a,z)\in E_2$,

$(v_2,v_3)\in E_1\leftrightarrow(f(v_2),\quad f(v_3))=(x,b)\in E_2$,

$(v_2,v_5)\in E_1\leftrightarrow(f(v_2),\quad f(v_5))=(x,c)\in E_2$,

$(v_3,v_4)\in E_1\leftrightarrow(f(v_3),\quad f(v_4))=(b,y)\in E_2$,

$(v_3,v_6)\in E_1\leftrightarrow(f(v_3),\quad f(v_6))=(b,z)\in E_2$,

$(v_4,v_5)\in E_1\leftrightarrow(f(v_4),\quad f(v_5))=(y,c)\in E_2$,

$(v_5,v_6)\in E_1\leftrightarrow(f(v_5),\quad f(v_6))=(c,z)\in E_2$,

从定义可知，如若$G_1\cong G_2$，必须满足。

(1) $|V(G_1)|=|V(G_2)|$， $|E(G_1)|=|E(G_2)|$。

(2) G_1 和 G_2 结点度的非增序列相同。

(3) 存在同构的导出子图。

其中(3)对判定两个图不同构有时十分有效。例如图 1.9 G_2 的结点集$\{a,b,c,d,e,f\}$所成的导出子图中有 2 个相邻的度为 3 的结点，其余结点的度均为 2。而 G_1 中却没有与之同构的导出子图，因此 G_1 与 G_2 不同构。

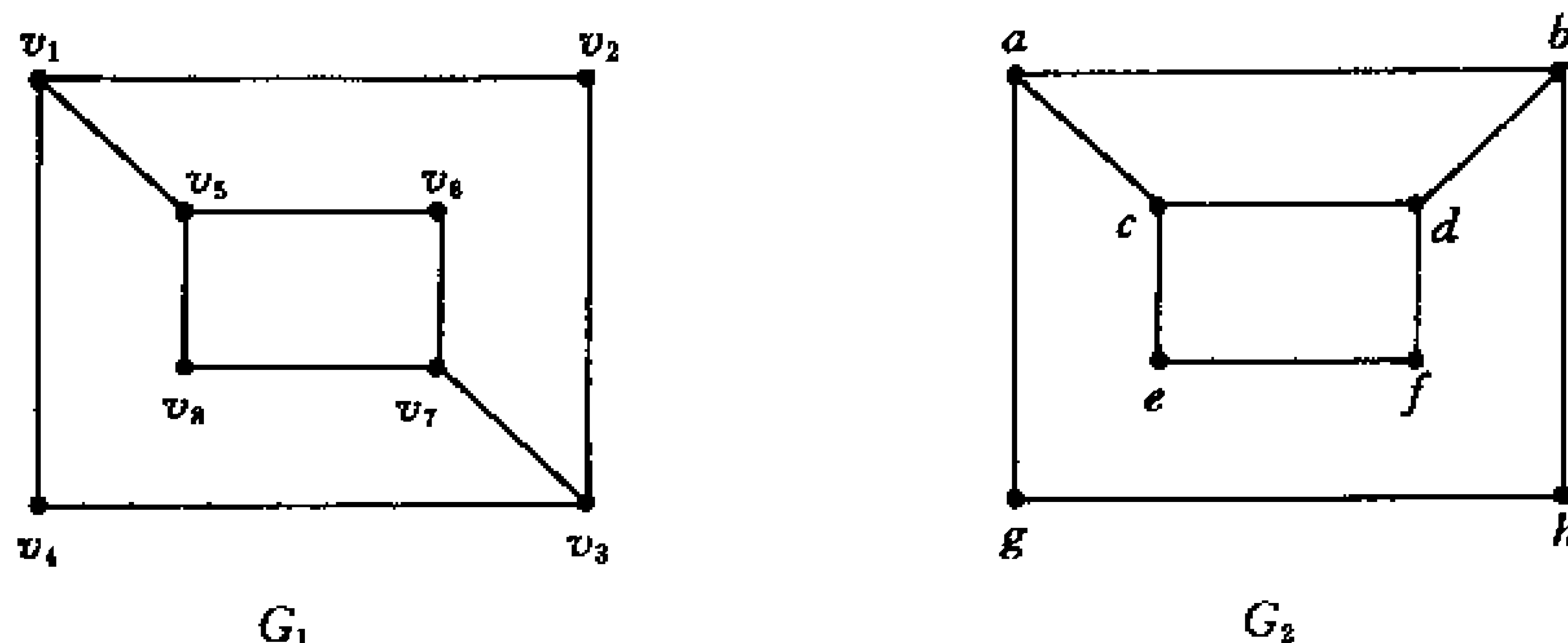


图 1.9

1.2 图的代数表示

在对图 G 进行描述或运算时，需要采用代数方法进行表示。常用的表示方法有

1.2.1 邻接矩阵

邻接矩阵表示了结点之间的邻接关系。

有向图的邻接矩阵 A 是一个 n 阶方阵，其元素为。

$$a_{ij}=\begin{cases}1, & (v_i,v_j)\in E。\\ 0, & 其它。\end{cases}$$

例如图 1.10 的邻接矩阵是

$$A=\begin{bmatrix}0&1&1&1&0\\0&0&1&0&1\\0&1&0&1&0\\0&0&0&0&0\\1&0&0&1&1\end{bmatrix}$$

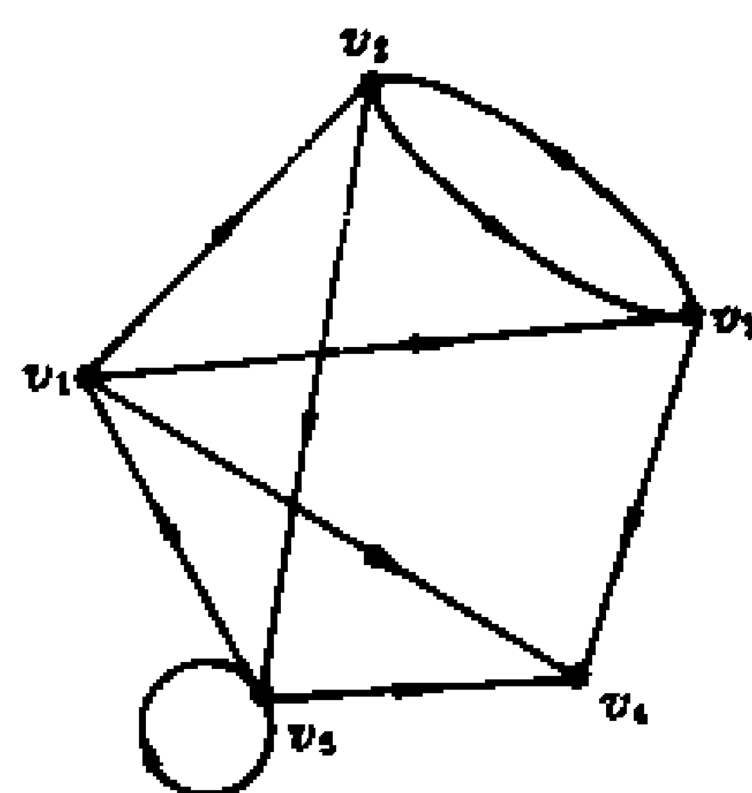


图 1.10

邻接矩阵 A 第 i 行非零元的数目恰是 v_i 的正度，第 j 列非零元的数目是 v_j 的负度。邻接矩阵可以表示自环，但无法表示重边。

无向图的邻接矩阵是一个对称矩阵，例如图 1.11 的邻接矩阵是

$$A=\begin{bmatrix}0&1&1&1&1\\1&0&1&0&1\\1&1&0&1&0\\1&0&1&0&1\\1&1&0&1&1\end{bmatrix}$$

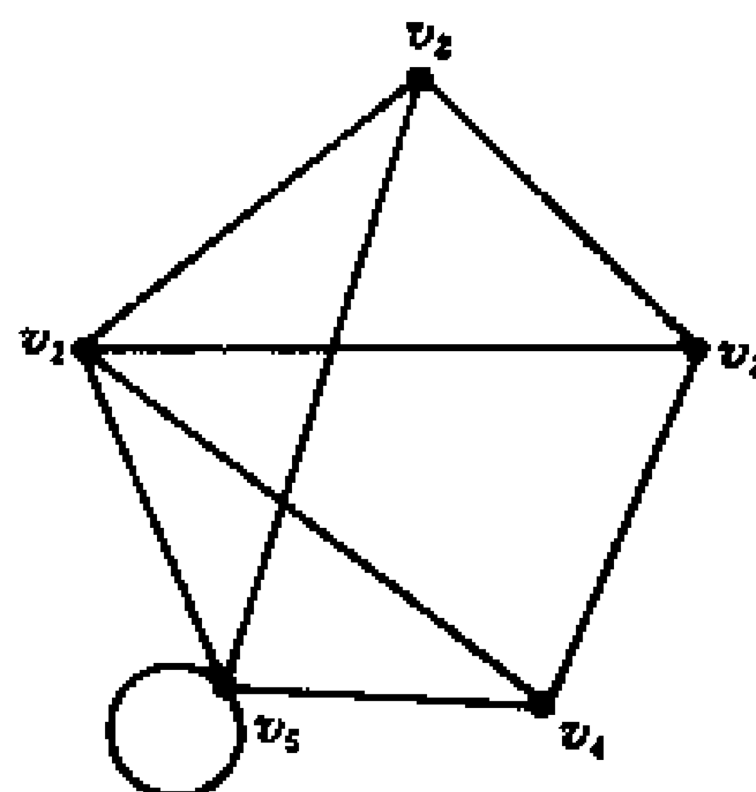


图 1.11

1.2.2 权矩阵

赋权图常用权矩阵 A 进行表示。其元素

$$a_{ij}=\begin{cases}w_{ij}, & (v_i,v_j)\in E。\\0, & 其它。\end{cases}$$

例如图 1.5 的权矩阵是

$$A=\begin{bmatrix}0&3&6&2&4\\3&0&4.2&0&5\\6&4.2&0&3&0\\2&0&3&0&7\\4&5&0&7&0\end{bmatrix}$$

1.2.3 关联矩阵

关联矩阵表示结点与边之间的关联关系。

有向图 G 的关联矩阵 B 是 $n\times m$ 的矩阵，当给定结点和边的编号之后，其元素

$$b_{ij}=\begin{cases}1, & e_j=(v_i,v_k)\in E。\\-1, & e_j=(v_k,v_i)\in E。\\0 & 其它。\end{cases}$$

例如图 1.12 的关联矩阵是

$$B=\begin{bmatrix} 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 1 & 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & -1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 1 \\ e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 \end{bmatrix}$$

图 1.12

关联矩阵具有以下性质：

1. 每列只有两个非零元：1 和 -1。

2. 第 i 行非零元的数目恰是结点 v_i 的度，其中 1 元的数目是 $d^+(v_i)$，-1 元的数目是 $d^-(v_i)$。

3. 能够表示重边，但不能表示自环。

类似地，无向图也有其关联矩阵 B，但其中不含 -1 元素。

例如图 1.13 的关联矩阵是

$$B=\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$e_1 \quad e_2 \quad e_3 \quad e_4 \quad e_5 \quad e_6 \quad e_7 \quad e_8 \quad e_9$

图 1.13

当邻接矩阵和关联矩阵能够表示某个图 G 时，这种表示是唯一的，而且十分直观。但由于它们不能表示重边或自环，因此这种表示有其局限性。特别在使用计算机对某个图 G 进行运算时，采用邻接矩阵或关联矩阵作为输入形式将占据较大的存储空间并可能增加计算复杂度。因此，为克服这些缺陷，再介绍图的另外几种常用表示方法。

1.2.4 边列表

边列表是对关联矩阵的列进行压缩的结果。它由两个 m 维向量 A 和 B 组成，当对 G 的结点和边分别编号之后，若 $e_k=(v_i,v_j)$，则 $A(k)=i$，$B(k)=j$，即 $A(k)$ 存放第 k 条边始点编号，$B(k)$ 存放其终点编号。如果 G 是赋权图，则再增加一个 m 维向量 Z，若 e_k 的权是 w_k，则令 $Z(k)=w_k$。例如图 1.14 的边列表示形式是

A：(4　4　1　2　2　2　4)

B：(1　1　2　2　4　3　3)

Z：(5　3　4　6　7　2　4)

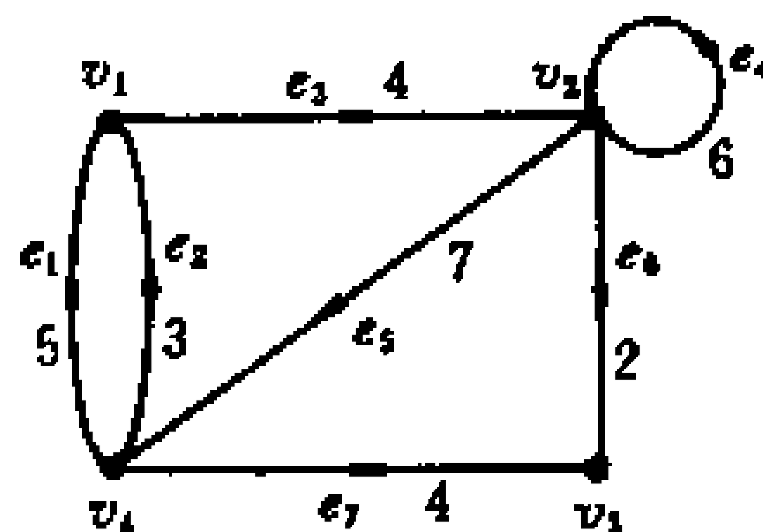


图 1.14

类似地可以得到无向图的边列表，比如图 1.15 的边列表是

A：(1　1　1　2　2　3)

B：(4　4　2　4　3　4)

Z：(5　3　4　7　2　4)

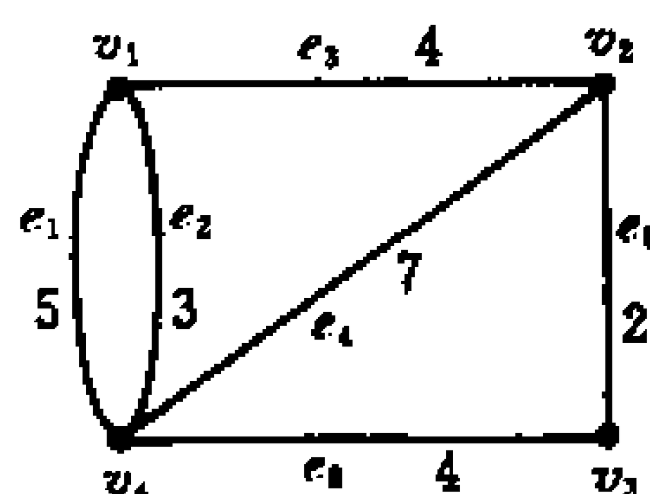
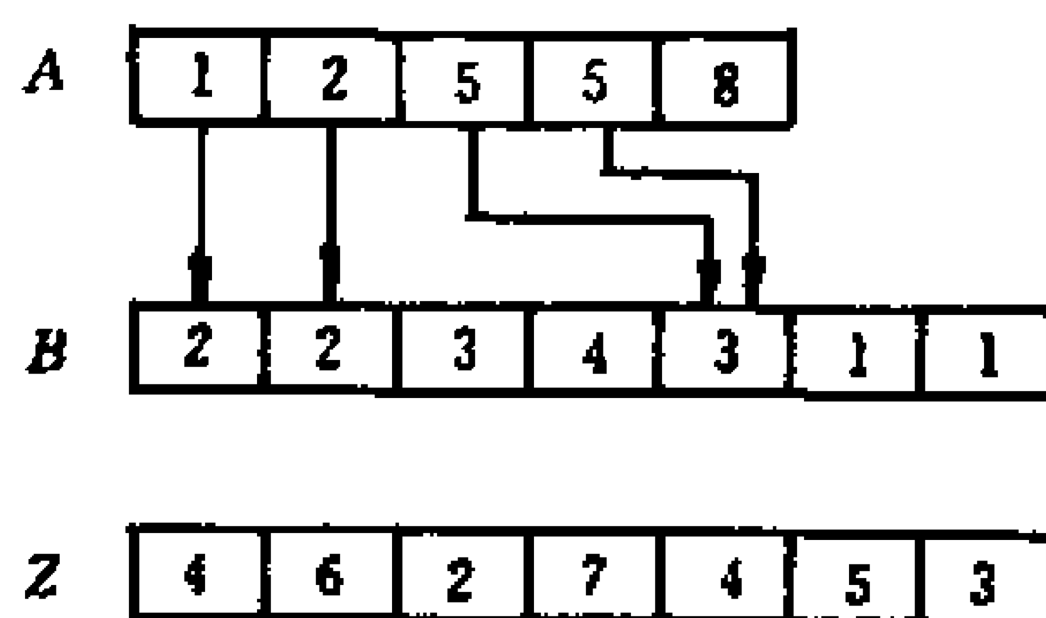


图　1.15

1.2.5　正向表

正向表是对邻接矩阵的行进行压缩的结果。它的特点是将每个结点的直接后继集中在一起存放。有向图的正向表由一个$(n+1)$维向量 A，一个 m 维向量 B 组成。当对 G 的结点编号之后，$A(i)$表示结点 v_i 的第一个直接后继在 B 中的地址，B 中存放这些后继结点的编号，$A(n+1)=m+1$。如果 G 是赋权图，则再设置一个 m 维向量 Z，用以存放相应的权值。例如图 1.14 的正向表是



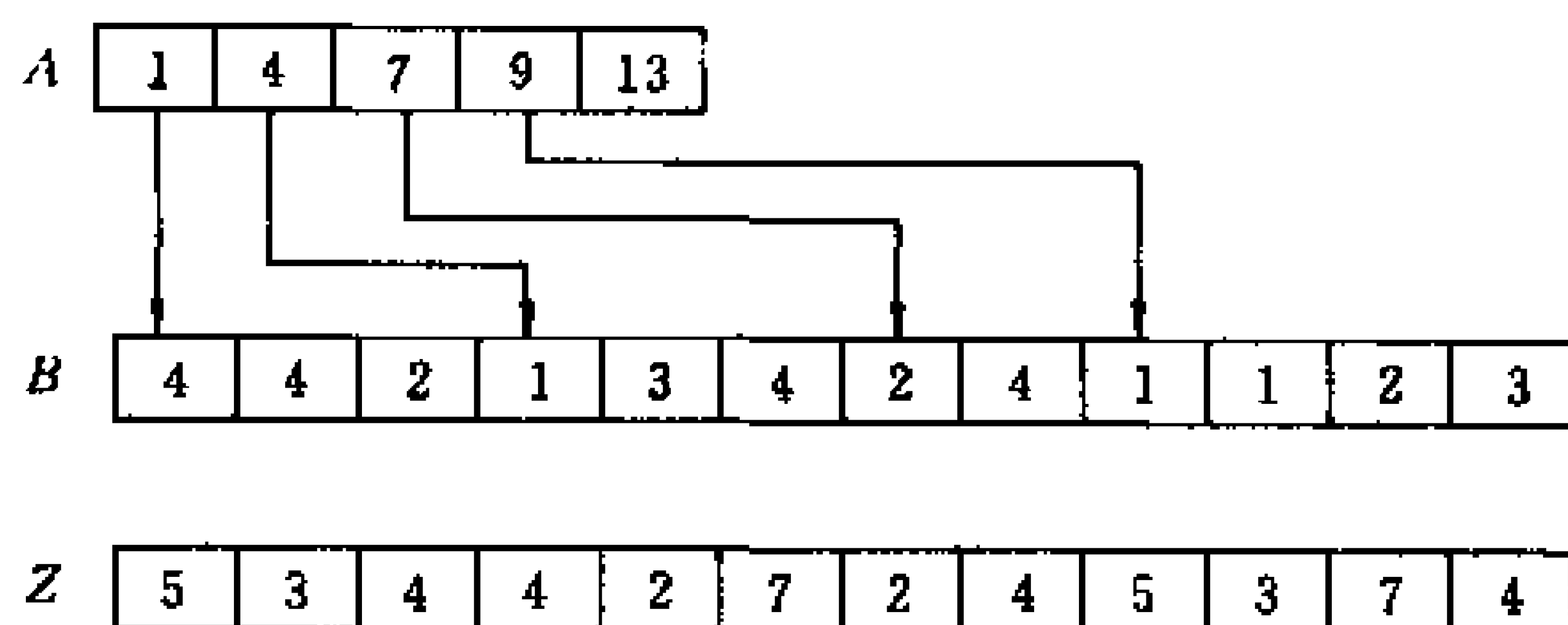
在正向表中存在下述关系：

1. $d^+(v_i)=A(i+1)-A(i)$

2. $A(i)=\sum_{j=1}^{i-1}d^+(v_j)+1$

3. 从 $B(A(i))$到 $B(A(i+1)-1)$的任一个值，都是 v_i 的直接后继。

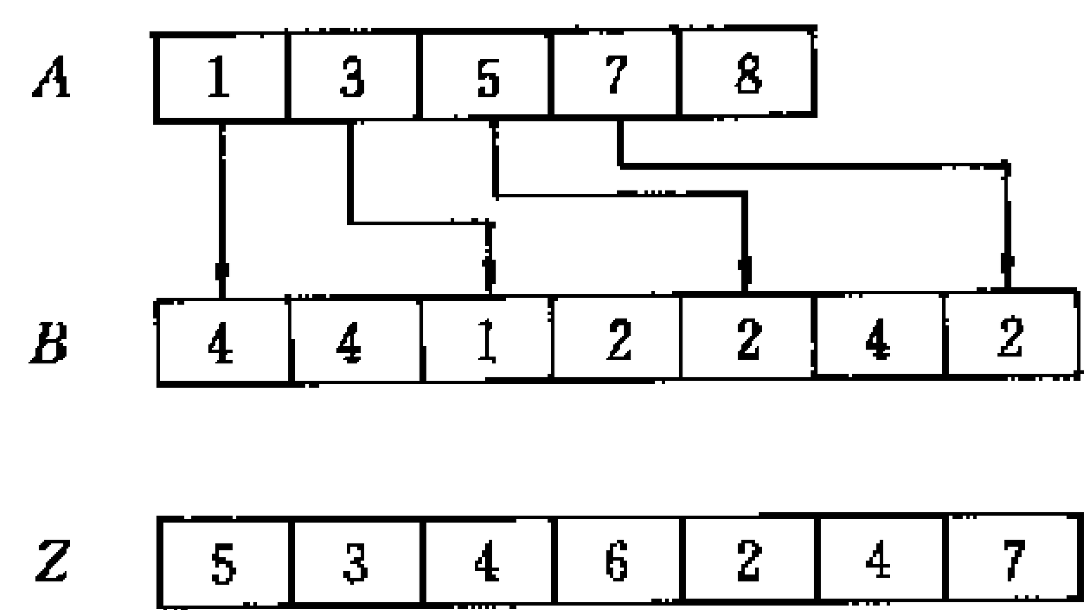
由于无向图的边没有方向性，所以 B 中存放的是相应邻接点的编号，因而 B 和 Z 都要扩充为 $2m$ 维的向量。例如图 1.15 的正向表是



1.2.6　逆向表

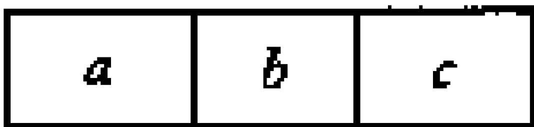
与正向表相反，逆向表是对有向图邻接矩阵的列进行压缩的结果。它的特点是将每个

结点的直接前趋集中在一起存放。例如图 1.14 的逆向表是。

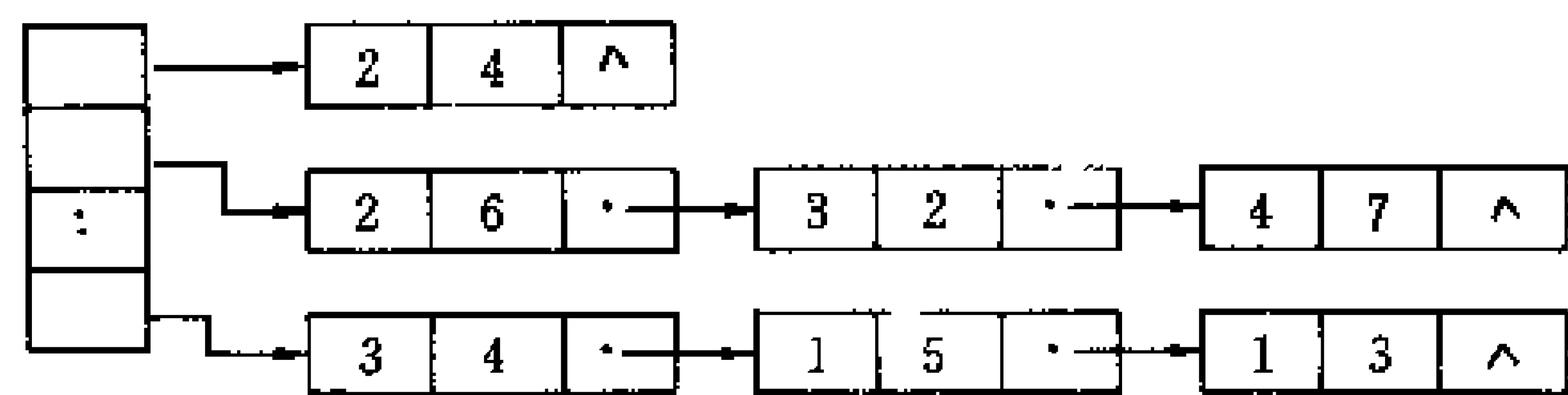


1.2.7 邻接表

这是采用单链表结构表示一个图。对每个结点 v_i 用一个表结点表示。在这里表结点的结构如下



它共分三个域，邻接点域 a 中存放该结点的编号，数据域 b 中存放相应边的数值，链域 c 中存放下一个表结点的地址指针。以图 1.14 为例，它的邻接表形式如下



其中 $Q(i)$ 存放结点 v_i 的第一个直接后继表结点的地址指针。邻接表的特点是使用灵活，比如要从图 G 中删去某条边时，只要摘除对应的表结点就可以实现；若要增加某条边，也只需增加一个表结点，而不需要进行大的变动。

边列表、正向表和邻接表等都能表示重边，也能表示自环。也就是说，它们都能唯一表示任意一个图。而且也都只占据较小的存储空间。邻接矩阵、关联矩阵、边列表、正向表、逆向表之间都可以互相转换。为了直观起见，本书主要采用邻接矩阵和关联矩阵表示图 G，在描述某些算法时，有时也采用正向表等形式的数据结构。

习 题 一

1. 证明在 9 座工厂之间，不可能每座工厂都只与其它 3 座工厂有业务联系，也不可能只有 4 座工厂与偶数个厂有业务联系。

2. 简单图 G 中，如果 $m>\frac{1}{2}(n-1)(n-2)$，证明 G 不存在孤立结点。

3. 完全图的每边任给一个方向，称为有向完全图。证明在有向完全图中

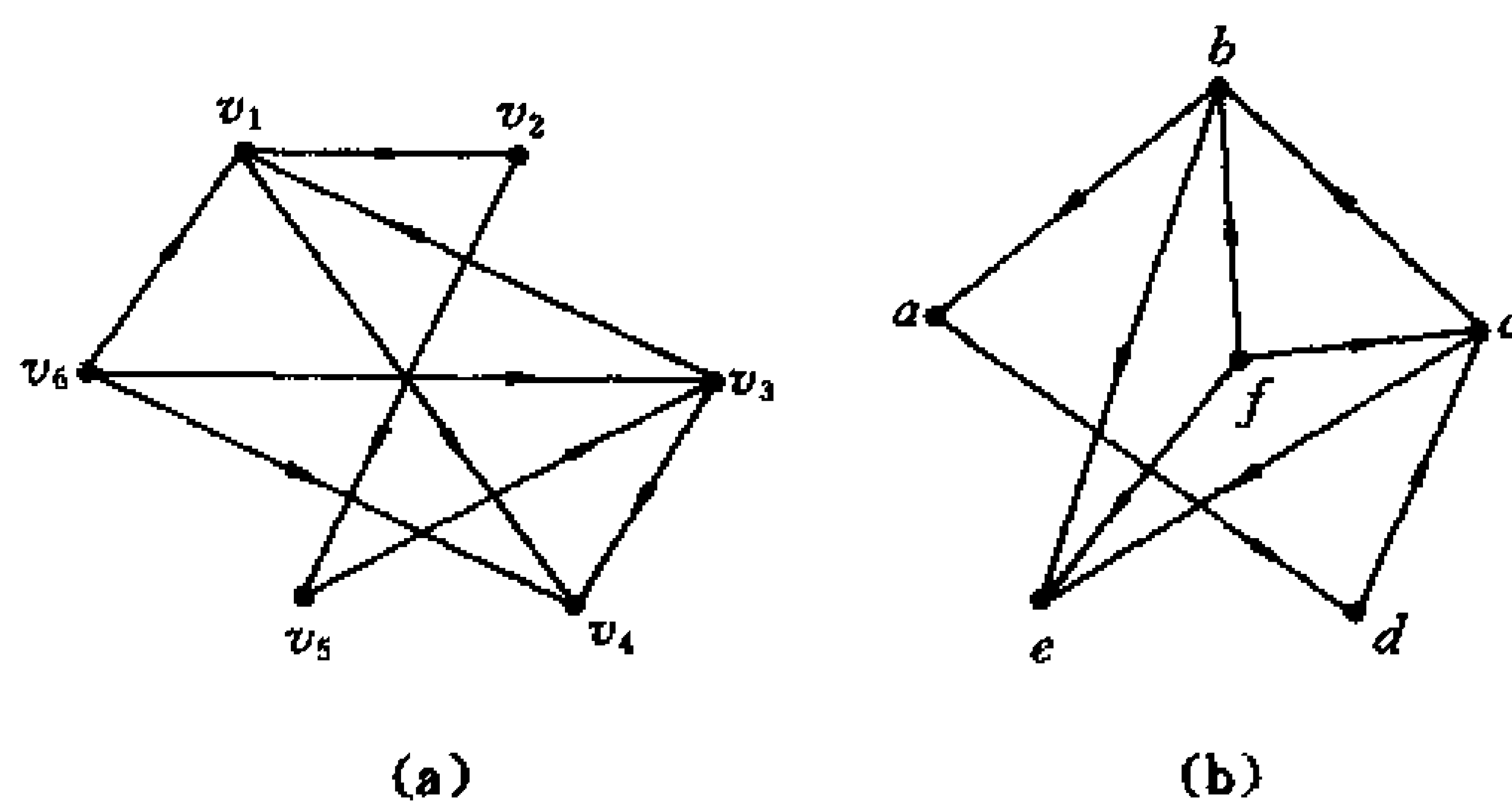
$$\sum_{v_i\in V}(d^+(v_i))^2=\sum_{v_i\in V}(d^-(v_i))^2。$$

4. 三个量杯容量分别是 8 升、5 升和 3 升，现 8 升的量杯装满了水，问怎样才能把水分成 2 个 4 升，画出相应的图。

5. 6个人围成圆形就座，每个人恰好只与相邻者不认识，是否可以重新入座，使每个人都与邻座认识？

6. 证明9个人中若非至少有4个人互相认识，则至少有3个人互相不认识。

7. 判断1.7图是否同构？



题图 1.7

8. 写出题1.7图(a)的邻接矩阵、关联矩阵，边列表及正向表。

9. 试编写有向图 G 的邻接矩阵与关联矩阵，邻接矩阵与正向表，关联矩阵与边列表之间互相转换的程序。

第二章　道路与回路

2.1　道路与回路

定义 2.1.1　有向图 $G=(V,E)$ 中，若边序列 $P=(e_{i1},e_{i2},\cdots,e_{iq})$，其中 $e_{ik}=(v_i,v_j)$ 满足 v_i 是 e_{ik-1} 的终点，v_j 是 e_{ik+1} 的始点，就称 P 是 G 的一条有向道路。如果 e_{iq} 的终点也是 e_{i1} 的始点，则称 P 是 G 的一条有向回路。

如果 P 中的边没有重复出现，则分别称为简单有向道路和简单有向回路。进而，如果在 P 中结点也不重复出现，又分别称它们是初级有向道路和初级有向回路简称为路和回路。显然，初级有向道路（回路）一定是简单有向道路（回路）

例 2.1.1　图 2.1 中，边序列 (e_5,e_4,e_5,e_7) 是有向道路，(e_5,e_4,e_5,e_7,e_3) 是有向回路。(e_5,e_4,e_1,e_2) 是简单有向道路，(e_5,e_4,e_1,e_2,e_3) 是简单有向回路。(e_1,e_2) 是初级有向道路，(e_1,e_2,e_3) 是初级有向回路。

定义 2.1.2　无向图 $G=(V,E)$ 中，若点边交替序列 $P=(v_{i1},e_{i1},v_{i2},e_{i2},\cdots,e_{iq-1},v_{iq})$ 满足 v_{ik},v_{ik+1} 是 e_{ik} 的两个端点，则称 P 是 G 中的一条链，或道路。如果 $v_{iq}=v_{i1}$，则称 P 是 G 中的一个圈，或回路。

如果 P 中没有重复出现的边，称之为简单道路或简单回路，若其中结点也不重复，又称之为初级道路或初级回路。

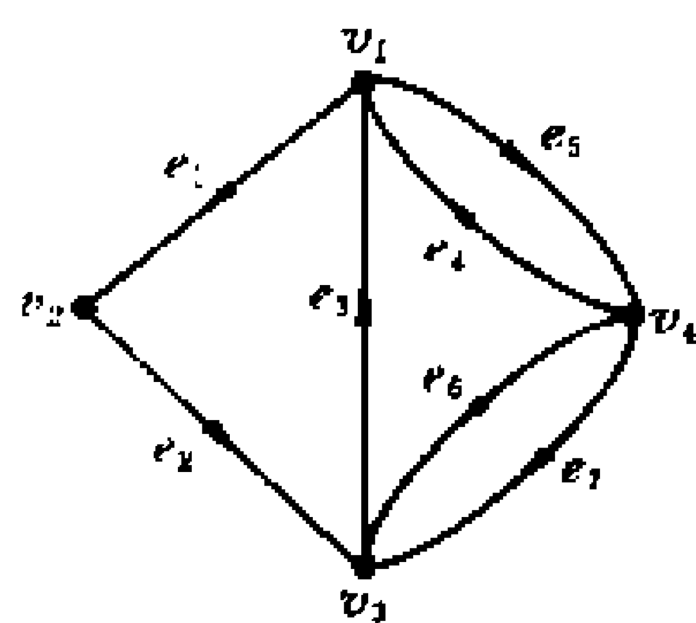


图　2.1

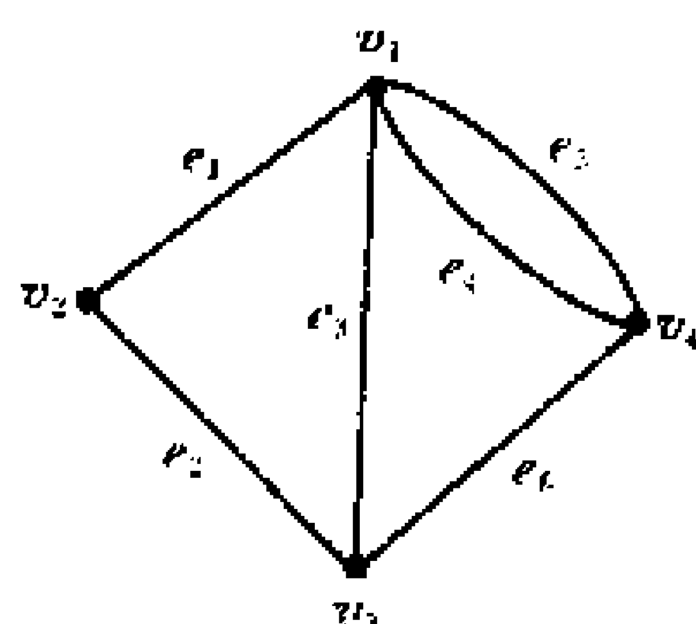


图　2.2

例 2.1.2　图 2.2 中边序列 (e_4,e_5,e_4,e_6) 是道路，(e_4,e_5,e_4,e_6,e_3) 是回路；(e_4,e_5,e_1,e_2) 是简单道路，(e_4,e_5,e_1,e_2,e_3) 是简单回路；(e_1,e_2) 是初级道路，(e_1,e_2,e_3) 是初级回路。

例 2.1.3　设 C 是简单图 G 中含结点数大于 3 的一个初级回路，如果结点 v_i 和 v_j 在 C 中不相邻，而边 $(v_i,v_j)\in E(G)$，则称 (v_i,v_j) 是 C 的一条弦。若对每一个 $v_k\in V(G)$，都有 $d(v_k)\geqslant 3$，则 G 中必含带弦的回路。

证明：在 G 中构造一条极长的初级道路 $P=(e_{i_1},e_{i_2},\cdots,e_{i_l})$，不妨设 $e_{i_1}=(v_0,v_1)$，$e_{i_l}=(v_{l-1},v_l)$。由于 P 是极长的初级道路，所以 v_0 和 v_l 的邻接点都在该道路 P 上。由已知条件，$d(v_0)\geqslant 3$，不妨设 $\Gamma(v_0)=\{v_1,v_{i_j},v_{i_k},\cdots\}$。其中 $1<j<k$，这时 $(v_0,v_1,\cdots,v_{i_k},v_0)$ 是一条初级回路，而 (v_0,v_{i_j}) 就是该回路中的一条弦。

例 2.1.4 设 $G=(V,E)$ 是无向图，如果 $V(G)$ 可以划分为子集 X 和 Y，使得对所有的 $e=(u,v)\in E(G)$，u 和 v 都分属于 X 或 Y，则称 G 是二分图。证明：如果二分图 G 中存在回路，则它们都是由偶数条边组成的。

证明：设 C 是二分图 G 的任一回路，不妨设 $v_0\in X$ 是 C 的始点，由于 G 是二分图，所以沿回路 C 必须经过偶数条边才能达到某结点 $v_i\in X$，因而只有经过偶数边才能回到 v_0。

定义 2.1.3 设 G 是无向图，若 G 的任意两结点之间都存在道路，就称 G 是连通图，否则称为非连通图。

如果 G 是有向图，不考虑其边的方向，即视之为无向图，若它是连通的，则称 G 是连通图。

若连通子图 H 不是 G 的任何连通子图的真子图，则称 H 是 G 的极大连通子图，或称连通支。显然 G 的每个连通支都是它的导出子图。

例 2.1.5 图 2.1 和 2.2 都是连通图，图 2.3 是非连通图。其中(a)有两个连通支，它们的结点集分别是 $\{v_1,v_2,v_3\}$ 和 $\{v_4,v_5\}$，(b)有三个连通支，其结点集是 $\{v_1,v_2,v_3\}$，$\{v_4,v_5\}$ 和 $\{v_6\}$。

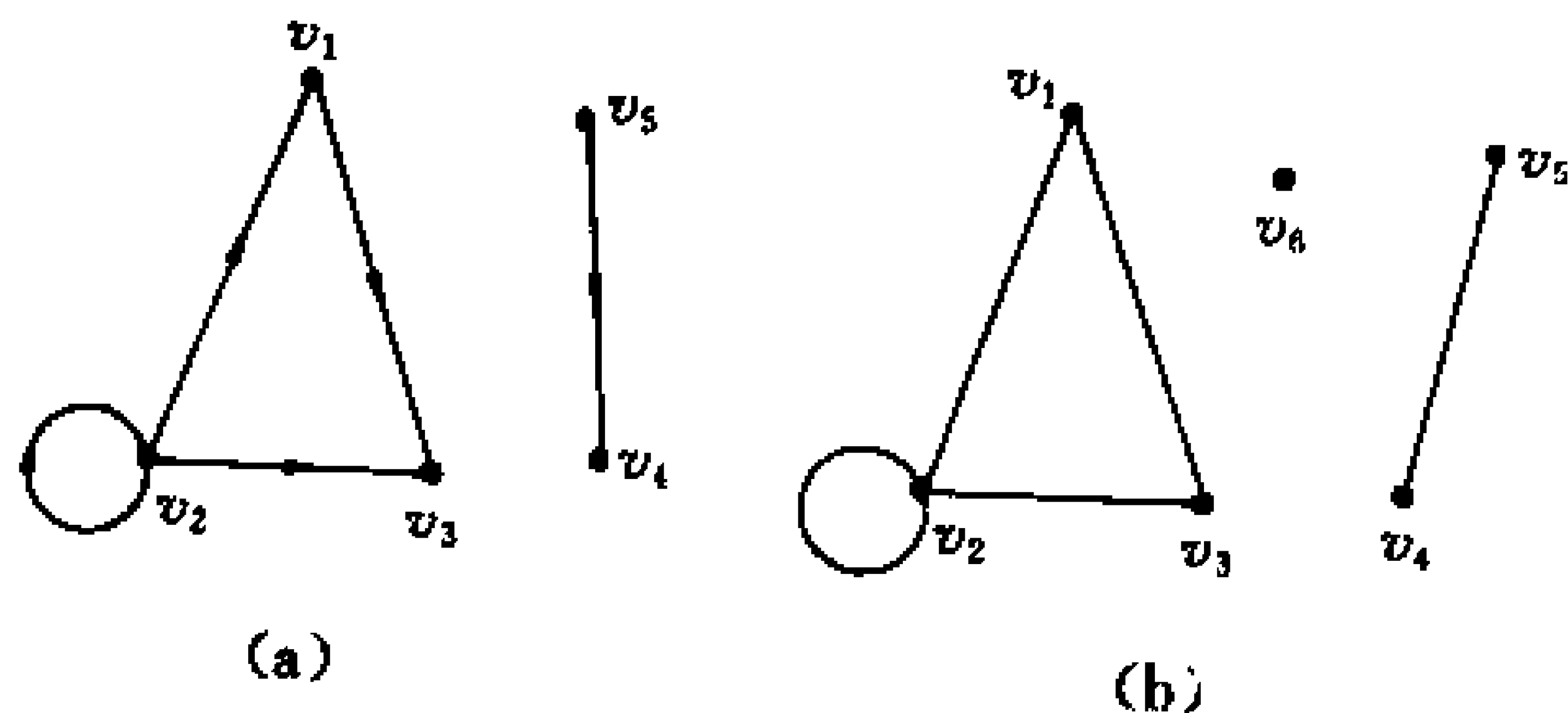


图 2.3

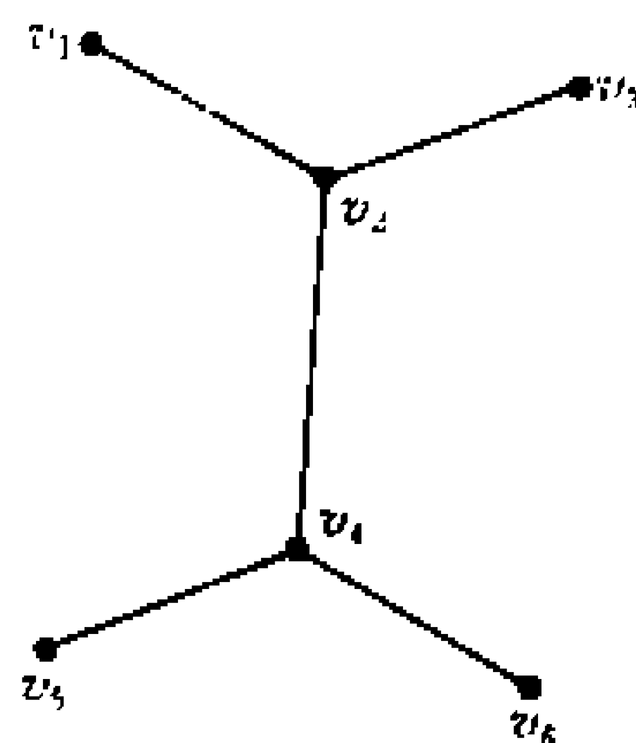


图 2.4

例 2.1.6 图 2.4 是连通图，它不含回路，而且在任意两结点之间都只有唯一的一条初级道路。这种图称为树，它是含边数最少的连通图。

例 2.1.7 设 G 是简单图，证明当 $m>\frac{1}{2}(n-1)(n-2)$ 时，G 是连通图。

证明：假定 G 是非连通图，则至少含有 2 个连通支。设分别为 $G_1=(V_1,E_1)$，$G_2=(V_2,E_2)$。其中 $|V_1(G_1)|=n_1$，$|V_2(G_2)|=n_2$。$n_1+n_2=n$。由于 G 是简单图，因此

$$|E_1(G_1)|\leqslant\frac{1}{2}n_1(n_1-1),$$

$$|E_2(G_2)|\leqslant\frac{1}{2}n_2(n_2-1),$$

$$m\leqslant\frac{1}{2}n_1(n_1-1)+\frac{1}{2}n_2(n_2-1)。$$

由于 $n_1\leqslant n-1$，$n_2\leqslant n-1$，

所以
$$\begin{aligned}m&\leqslant\frac{1}{2}(n-1)(n_1-1+n_2-1)\\&=\frac{1}{2}(n-1)(n-2),\end{aligned}$$

与已知条件矛盾，故 G 是连通图。

2.2　道路与回路的判定

通常可以利用邻接矩阵或搜索法判定某个图 G 的两结点间是否存在道路，或者判定它是否连通。首先介绍邻接矩阵的判定方法。

设 $A=(a_{ij})_{n\times n}$是 G 的邻接矩阵。由 A 的定义，$a_{ij}=1$ 表示$(v_i,v_j)\in E(G)$，即 v_i 可以通过某条边 e 到达 v_j，或者说 G 中有道路从 v_i 到 v_j。根据矩阵乘法，设 $A^2=(a_{ij}^{(2)})$，有

$$a_{ij}^{(2)}=\sum_{k=1}^{n}a_{ik}\cdot a_{kj}。$$

$a_{ij}^{(2)}\neq 0$ 当且仅当存在 k，使 $a_{ik}=a_{kj}=1$。也就是说，如果 G 中存在结点 v_k，满足(v_i,v_k)，$(v_k,v_j)\in E(G)$，即经过 2 条边(v_i,v_k)，(v_k,v_j)，v_i 可以到达 v_j 时，$a_{ij}^{(2)}\neq 0$。同理，$A^l(l\leqslant n)$中的元素 $a_{ij}^{(l)}\neq 0$ 表示了 v_i 可以经过 l 条边到达 v_j。因此令

$$P=A+A^2+\cdots+A^n,$$

如果 $p_{ij}=t$，说明 v_i 有 t 条道路可以到达 v_j。若 $p_{ij}=0$，即 n 步之内 v_i 不能到达 v_j，则在 G 中不存在 v_i 到 v_j 的路。否则，若 v_i 经过 $l(l>n)$步可达 v_j，由抽屉原理，该道路上一定存在重复出现的结点 v_k，而 v_k 之间的这段路 C 是一个回路。删去这段回路 v_i 仍然可达 v_j。由于 G 中只存在 n 个不同的结点，所以只要 v_i 有道路到 v_j，一定有 $p_{ij}\neq 0$。

在许多实际问题中，往往只要求了解 v_i 与 v_j 之间是否存在道路。对此可以采用逻辑运算的方法，即

$$a_{ij}^{(l)}=\bigvee_{k=1}^{n}(a_{ik}^{(l-1)}\wedge a_{kj}),\qquad l=2,3,\cdots,n。$$

相应地

$$P=A\vee A^2\vee\cdots\vee A^n$$

就是图 G 的道路矩阵。

用上述方法求 G 的道路矩阵，计算复杂性为 $O(n^4)$。以下介绍的 Warshall 算法是一个更好的方法，其计算复杂性是 $O(n^3)$。

Warshall 算法

```
begin
1. P←A,
2. for i=1 to n do
3.     for j=1 to n do
4.           for k=1 to n do
                  pjk←pjk ∨ (pji ∧ pik)。
end.
```

例 2.2.1　采用 Warshall 算法计算图 2.5 道路矩阵的过程是：

$$P\leftarrow\begin{bmatrix}0&1&1&0&0\\0&0&1&1&0\\0&0&0&0&1\\0&0&0&0&0\\1&0&0&1&0\end{bmatrix}$$

$$P(i=1)=\begin{bmatrix}0&1&1&0&0\\0&0&1&1&0\\0&0&0&0&1\\0&0&0&0&0\\1&\mathbf{1}&\mathbf{1}&1&0\end{bmatrix}\qquad P(i=2)=\begin{bmatrix}0&1&1&\mathbf{1}&0\\0&0&1&1&0\\0&0&0&0&1\\0&0&0&0&0\\1&1&1&1&0\end{bmatrix}$$

$$P(i=3)=\begin{bmatrix}0&1&1&1&\mathbf{1}\\0&0&1&1&\mathbf{1}\\0&0&0&0&1\\0&0&0&0&0\\1&1&1&1&\mathbf{1}\end{bmatrix}\qquad P(i=4)=P(i=3),$$

$$P(i=5)=\begin{bmatrix}\mathbf{1}&1&1&1&1\\\mathbf{1}&\mathbf{1}&1&1&1\\\mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{1}&1\\0&0&0&0&0\\1&1&1&1&1\end{bmatrix}$$

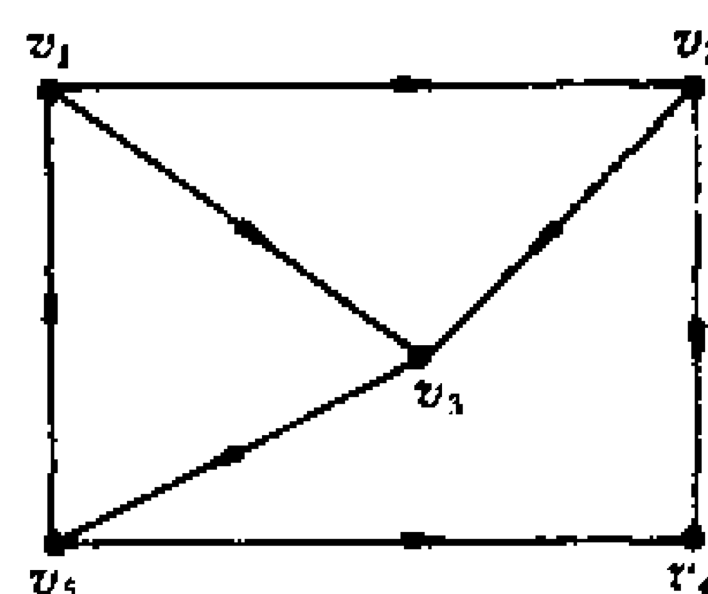


图 2.5

矩阵 P 中的粗体字表示该元素的值在本次循环中发生改变。

定理 2.2.1 Warshall 算法的结果是图 G 的道路矩阵。

证明：该定理的严格证明需要对三层循环分别使用归纳法。现只证其最外层循环。

基始：当 $i=1$ 时，

$p_{jk}^{(1)}=p_{jk}\vee(p_{j1}\wedge p_{1k})$，$k=1,2,\cdots,n$；$j=1,2,\cdots,n$。

$p_{jk}^{(1)}=1$ 当且仅当 $p_{jk}=1$ 或 $p_{j1}=p_{1k}=1$，其中 $p_{jk}=1$ 表明 v_j 直接可达 v_k，$p_{j1}=p_{1k}=1$ 表明 v_j 可以经过 v_1 到达 v_k。因此 $p_{jk}^{(1)}=1$ 当且仅当结点集$\{v_j,v_1,v_k\}$之间有 v_j 到 v_k 的路。

$i=2$ 时，$p_{jk}^{(2)}=p_{jk}^{(1)}\vee(p_{j2}^{(1)}\wedge p_{2k}^{(1)})$，$k=1,2,\cdots,n$；$j=1,2,\cdots,n$。$p_{jk}^{(2)}=1$ 当且仅当 $p_{jk}^{(1)}=1$ 或 $p_{j2}^{(1)}=p_{2k}^{(1)}=1$，其中 $p_{jk}^{(1)}=1$ 表明结点集$\{v_j,v_1,v_k\}$之间有 v_j 到 v_k 的道路；$p_{j2}^{(1)}$和 $p_{2k}^{(1)}$为 1 表明$\{v_j,v_1,v_2,v_k\}$之间 v_j 有必通过 v_2 到达 v_k 的道路，因此，$p_{jk}^{(2)}=1$ 当且仅当结点集$\{v_j,v_1,v_2,v_k\}$中有 v_j 到 v_k 的道路。

设 $i=n-1$ 时，$p_{jk}^{(n-1)}=1$ 当且仅当结点集 $\{v_j,v_1,v_2,\cdots,v_{n-1},v_k\}$ 之中有 v_j 到 v_k 的道路。

则 $i=n$ 时，$p_{jk}^{(n)}=p_{jk}^{(n-1)}\vee(p_{jn}^{(n-1)}\wedge p_{nk}^{(n-1)})$，

$k=1,2,\cdots,n$，$j=1,2,\cdots,n$。

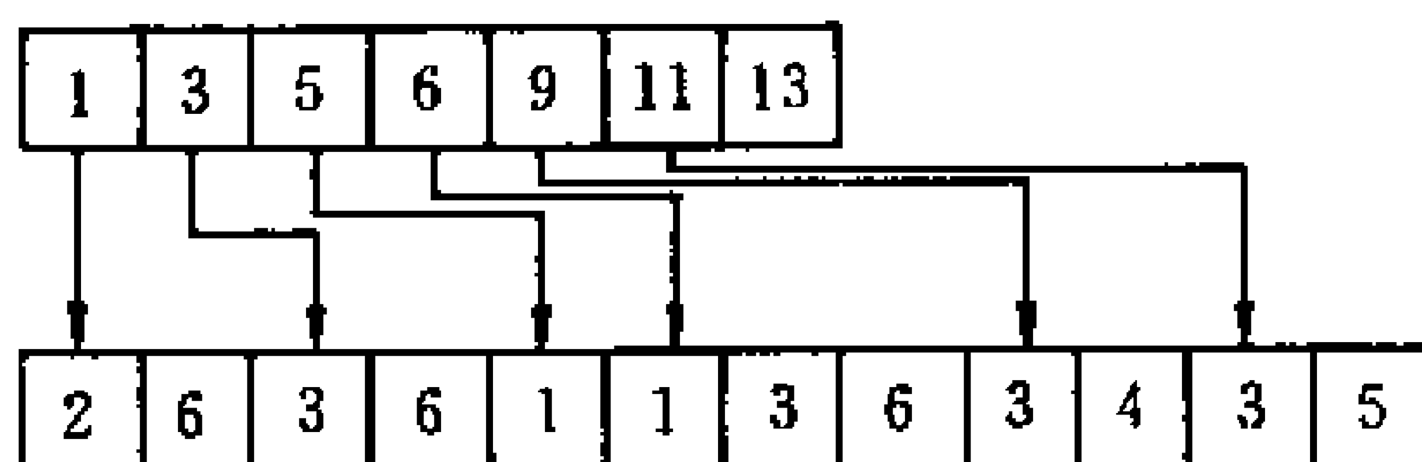
由归纳假设，$p_{jk}^{(n-1)}$表明结点集$\{v_j,v_1,\cdots,v_{n-1},v_k\}$中有 v_j 到 v_k 的路，$p_{jn}^{(n-1)}=p_{nk}^{(n-1)}=1$，表明结点集$\{v_j,v_1,\cdots,v_{n-1},v_n,v_k\}$中 v_j 有通过 v_n 到达 v_k 的道路。因此，$p_{jk}^{(n)}=1$ 即是结点集$\{v_j,v_1,\cdots,v_n,v_k\}$之中有 v_j 到 v_k 的道路。

采用搜索的方法判断 G 中某一结点 v_0 到另一结点 v_j 是否存在道路经常更加方便。常用的搜索法有广探法(Breadth First Search)和深探法(Depth First Search)。

广探法(BFS)是从 G 的任一结点 v_0 开始，找它的直接后继集 $\Gamma^+(v_0)$，记为 A_1，然后对 A_1 中的每一结点分别找它们的直接后继集，这些直接后继集的并记为 A_2。依此类推，直至达到目的。为了避免结点的重复搜索，可以首先对全部结点都给一个标记"0"，当 v_i 被搜索到时，如果其标记为 0，则 v_i 进入直接后继集，同时标记改为 1，否则由于 v_i 已被搜索因此不再进入直接后继集。

例 2.2.2 用 BFS 方法找图 2.6 中 v_1 到 v_4 的一条道路。

解：如果采用正向表的输入结构，则有



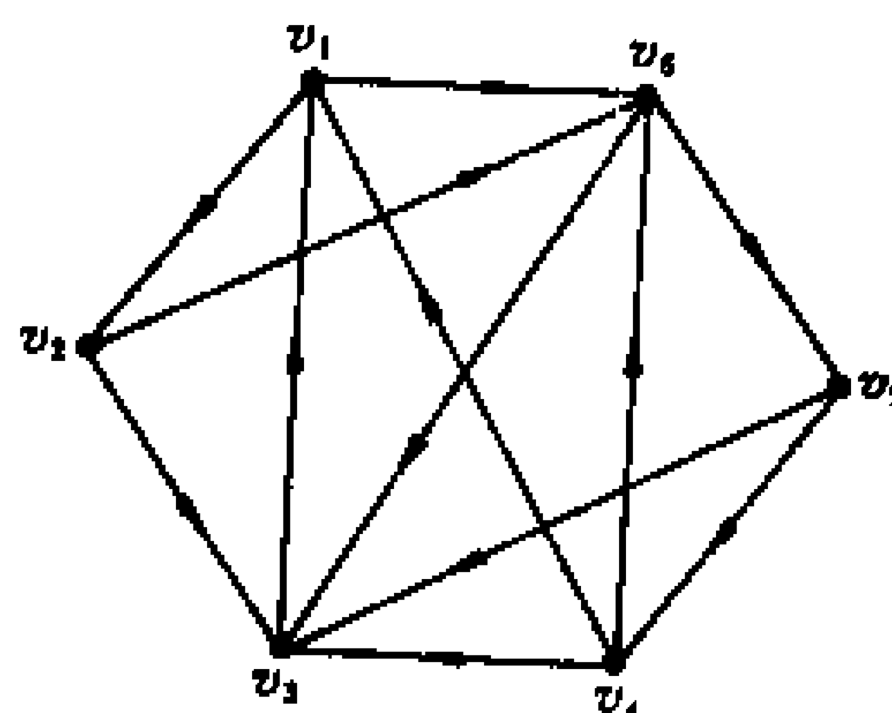


图 2.6

$\because\ \Gamma^+(v_1)=\{v_2,v_6\}$，　　$\therefore\ A_1=\{v_2,v_6\}$。

$\because\ \Gamma^+(v_2)=\{v_3,v_6\}$，

$\Gamma^+(v_6)=\{v_3,v_5\}$

$\therefore\ A_2=\{v_3,v_5\}$。

$\because\ \Gamma^+(v_3)=\{v_1\}$，

$\Gamma^+(v_5)=\{v_3,v_4\}$，

$\therefore\ A_3=\{v_4\}$。

因此 G 中存在 v_1 到 v_4 的道路。

从上例中可知，用 BFS 方法求两点间道路的计算复杂性是 $O(m)$。

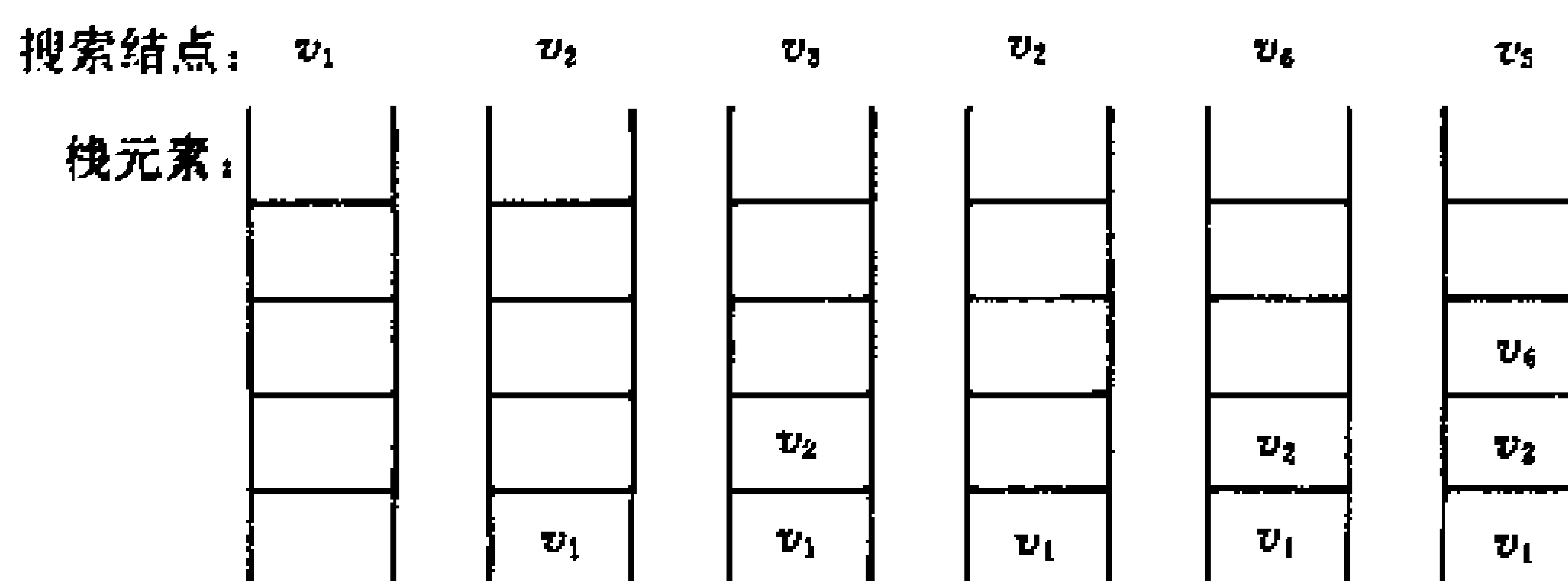


图 2.7

深探法(DFS)的特点与 BFS 截然不同。它从某一结点 v_0 开始，只查找 v_0 的某个直接后继 v_1，记下 v_1 的父亲 v_0，然后再找 v_1 的某个未搜索过的直接后继 v_2。依此类推。当从某个结点 v_j 无法再向下搜索时，退回到它的父亲 v_{j-1}，然后再找 v_{j-1} 的另一个未查过的直接后继。形象地说，DFS 的特点是尽量向下搜索，只有碰壁才回头。

采用栈结构以及前述的标记结点的方法可以完成 DFS 的搜索过程。

例 2.2.3 用 DFS 方法找图 2.6 中 v_1 到 v_4 的一条道路。

解：数据输入依然采用正向表。v_1 的第一个直接后继是 v_2，v_1 进栈；v_2 的第一个后继是 v_3，v_2 进栈。v_3 的后继是 v_1，但已标记，故退栈。v_2 的另一个后继是 v_6，v_2 进栈；v_6 的第 1 个后继是已标记结点 v_3，第 2 个后继是 v_5，v_6 进栈。v_5 的后继是 v_4。至此，已搜索到 v_1 到 v_4 的一条道路。整个搜索过程可用图 2.7 形象地表示。其计算复杂性也是 $O(m)$。

2.3 欧拉道路与回路

1736 年瑞士著名数学家欧拉(Leonhard Euler)发表了图论的第一篇论文"哥尼斯堡七桥问题"。这个问题是这样的：哥尼斯堡城被 Pregel 河分成了 4 部分，它们之间有 7 座桥。如图 2.8 所示。当时人们提出了一个问题，能否从城市的某处出发，过每座桥一次且仅一次最后回到原处。欧拉的文章漂亮地解决了这个问题。他把 4 块陆地设想为 4 个结点，分别用 A、B、C、D 表示，而将桥画成相应的边，如图 2.9。于是问题转化为在该图中是否存在经过每条边一次且仅一次的回路。欧拉的论文给出了解决这类问题的准则，并对七桥问题给出了否定的结论。

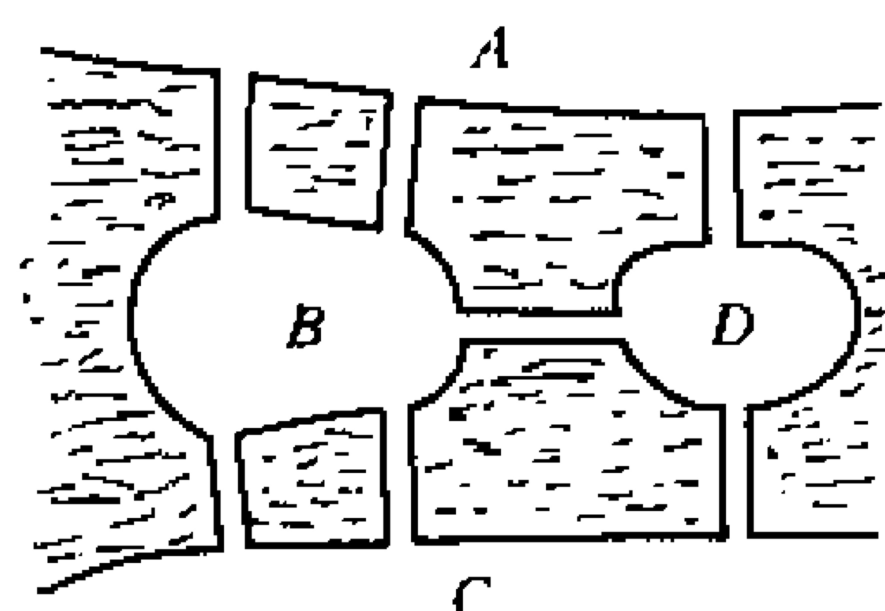


图 2.8

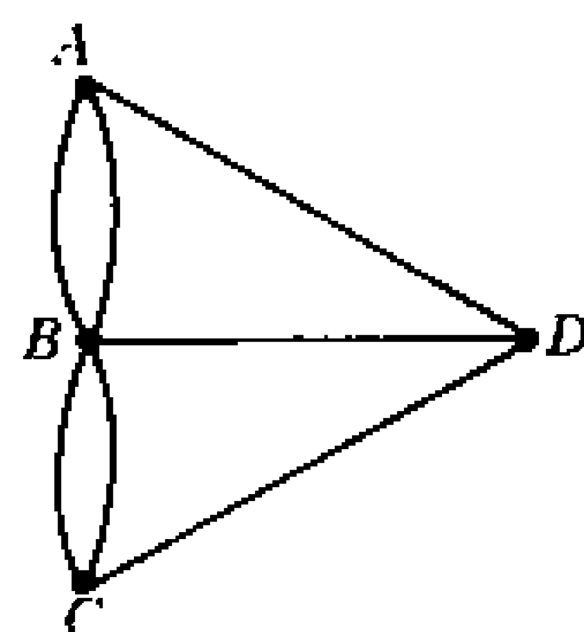


图 2.9

定义 2.3.1 无向连通图 $G=(V,E)$ 中的一条经过所有边的简单回路(道路)称为 G 的欧拉回路(道路)。

定理 2.3.1 无向连通图 G 存在欧拉回路的充要条件是 G 中各结点的度都是偶数。

证明：必要性。若 G 中有欧拉回路 C，则 C 过每一条边一次且仅一次。对任一结点 v 来说，如果 C 经由 e_i 进入 v，则一定通过另一条边 e_j 从 v 离开。因此结点 v 的度是偶数。

充分性。由于 G 是有穷图，因此可以断定，从 G 的任一结点 v_0 出发一定存在 G 的一条简单回路 C。这是因为各结点的度都是偶数，所以这条简单道路不可能停留在 v_0 以外的某个结点，而不能再向前伸延以至构成回路 C。

如果 $E(G)=C$，则 C 就是欧拉回路，充分性得证。否则在 G 中删去 C 的各边，得到 $G_1=G-C$。G_1 可能是非连通图，但每个结点的度保持为偶数。这时，G_1 中一定存在某个度非零的结点 v_i，同时 v_i 也是 C 中的结点。否则 C 的结点与 G_1 的结点之间无边相连，与 G 是连通图矛盾。同样理由，从 v_i 出发，G_1 中 v_i 所在的连通支内存在一条简单回路 C_1。显然 $C\cup C_1$ 仍然是 G 的一条简单回路，但它包括的边数比 C 多。继续以上构造方法，最终有简单回路 $C'=C\cup C_1\cup\cdots\cup C_k$，它包含了 G 的全部边，即 C' 是 G 的一条欧拉回路。

以上采用了构造性证明的方法，即证明过程本身就给出了问题求解的步骤。

例 2.3.1 试找出图 2.10 的一条欧拉回路。

解：从任一点，比如 v_1 开始，可构造简单回路 $C=(e_1,e_6,e_8,e_7,e_2)$。$G_1=G-C$ 中的 v_2,v_5 度非零且是 C 中的结点，从 v_2 开始 G_1 中有简单回路 $C_1=(e_3,e_5,e_4)$。因此 $C\cup C_1=(e_1,e_3,e_5,e_4,e_6,e_8,e_7,e_2)$ 包含了 G 的所有边，即是 G 的一条欧拉回路。

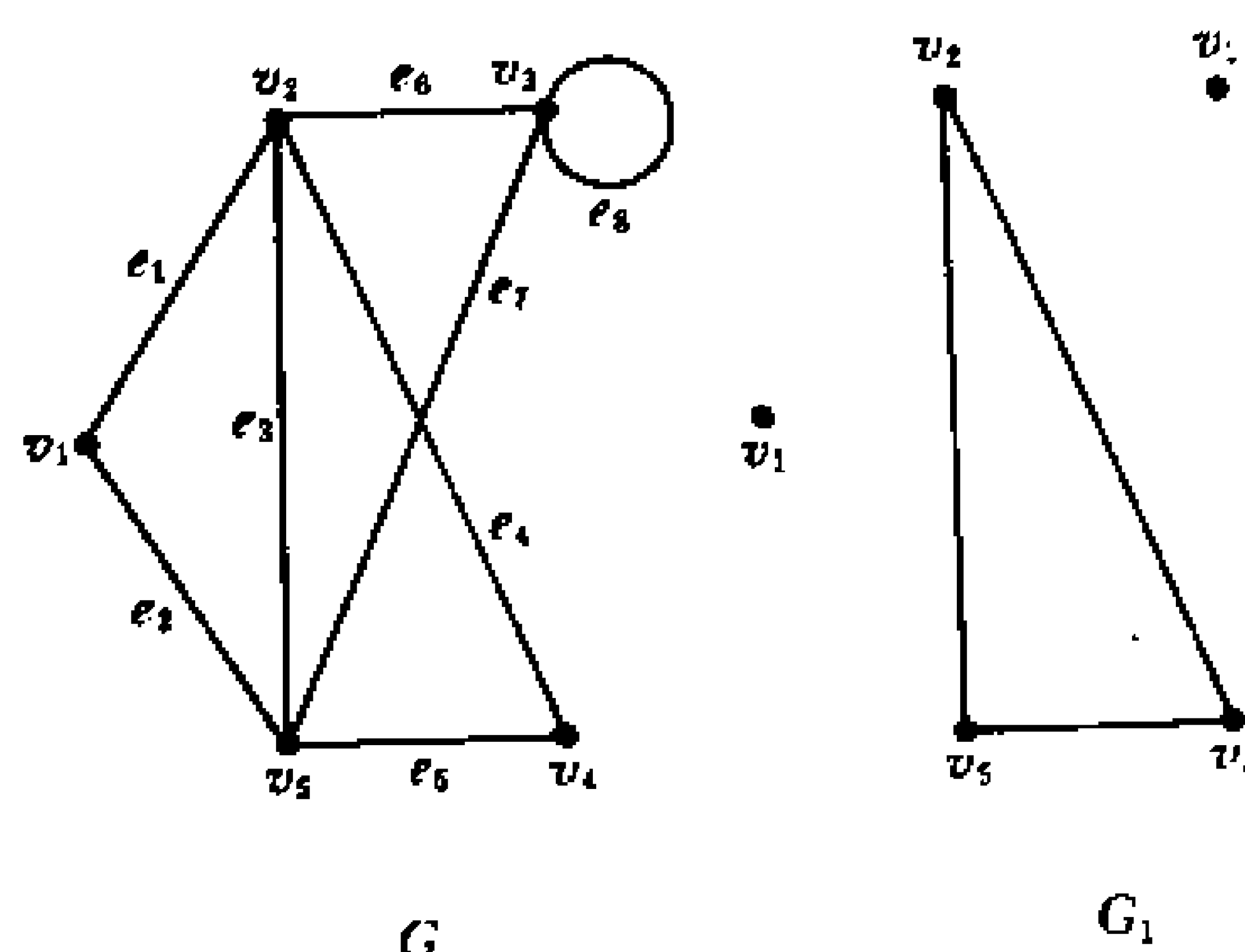


图 2.10

推论 2.3.1 若无向连通图 G 中只有 2 个度为奇的结点，则 G 存在欧拉道路。

证明：设 v_i 和 v_j 是两个度为奇数的结点。作 $G'=G+(v_i,v_j)$，则 G' 中各点的度都是偶数。由定理 2.3.1，G' 有欧拉回路，它包含边 (v_i,v_j)，删去该边，得到一条从 v_i 到 v_j 的简单道路，它恰好经过了 G 的所有边，亦即是一条欧拉道路。

推论 2.3.2 若有向连通图 G 中各结点的正、负度相等，则 G 存在有向欧拉回路。

其证明与定理 2.3.1 的证明相仿。

例 2.3.2 七桥问题中既不存在欧拉回路也不存在欧拉道路

例 2.3.3 设连通图 $G=(V,E)$ 有 k 个度为奇数的结点，证明 $E(G)$ 可以划分成 $k/2$ 条简单道路。

证明：由性质 1.1.2，k 是偶数。在这 k 个结点间增添 $k/2$ 条边，使每个结点都与其中一条边关联，得到 G'，G' 中各结点的度都为偶数。由定理 2.3.1，G' 中有欧拉回路 C，这 $k/2$ 条边都在 C 上且不相邻接。删去这些边，得到 $k/2$ 条简单道路，它们包含了 G 的所有边。亦即 $E(G)$ 划分成了 $k/2$ 条简单道路。

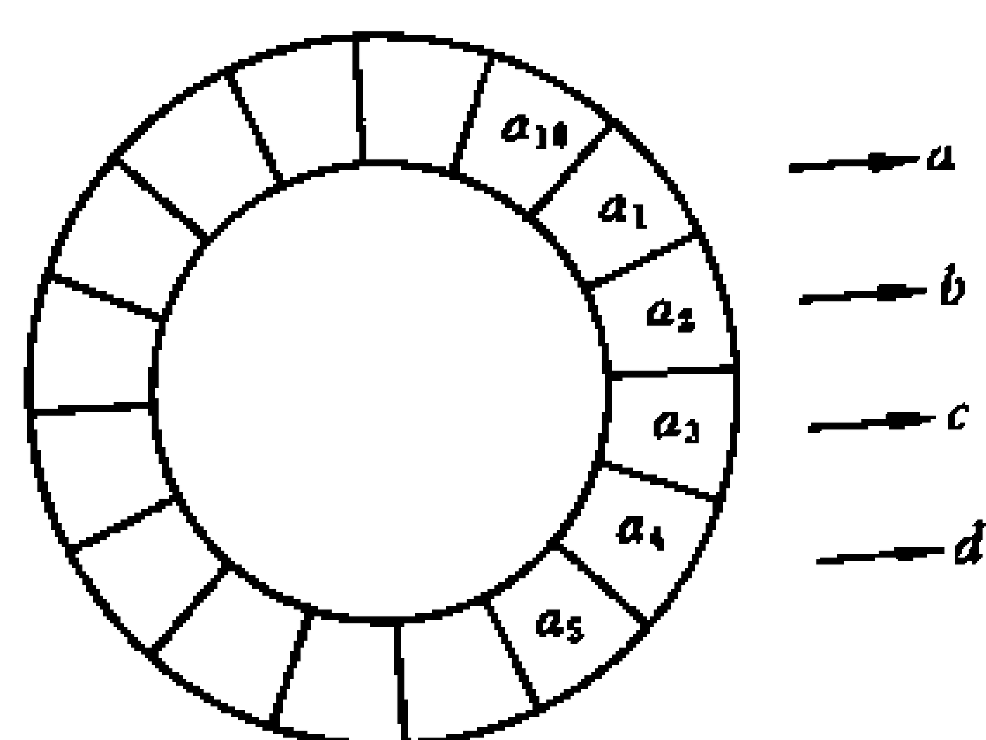


图 2.11

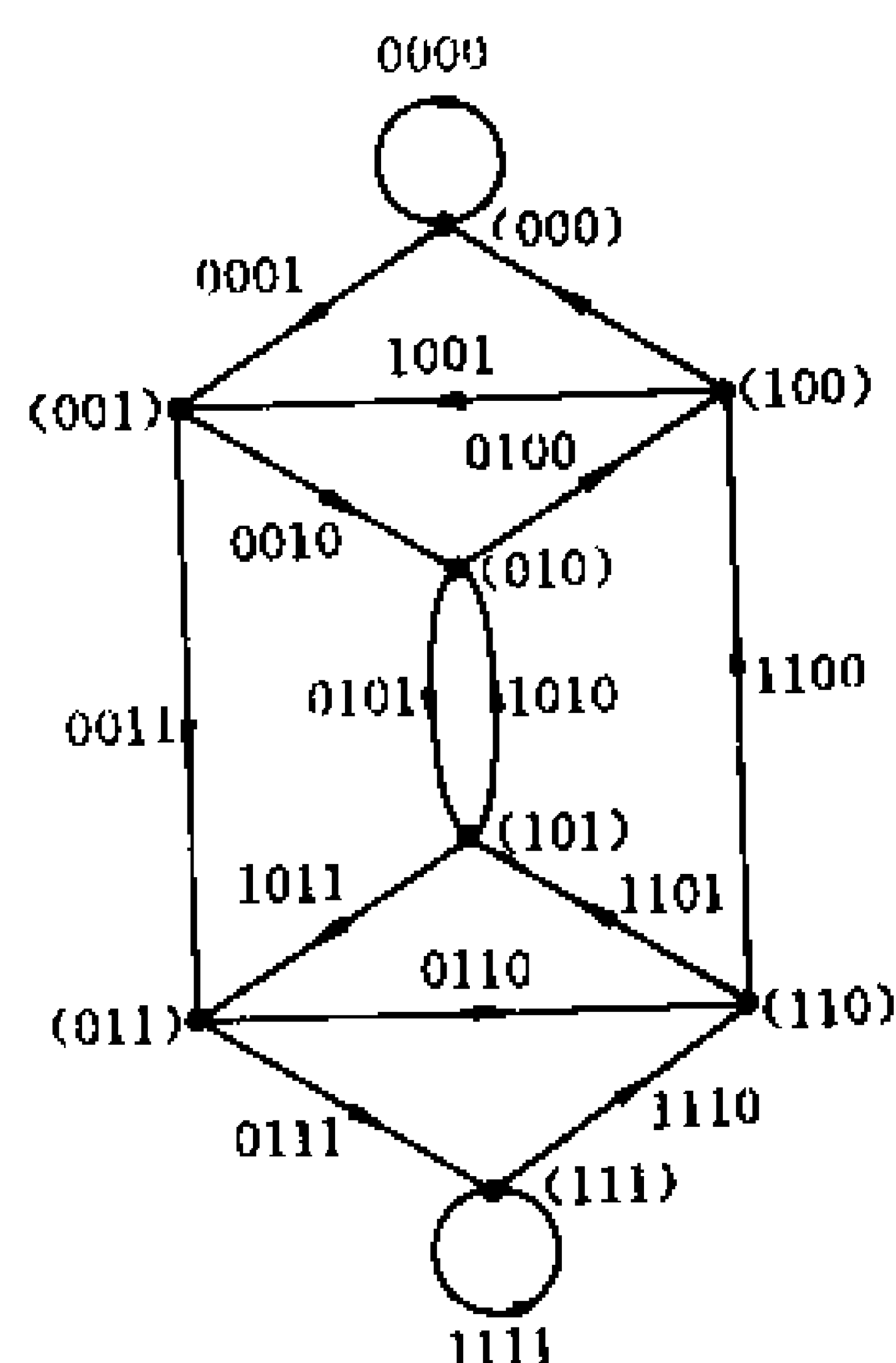


图 2.12

例 2.3.4 一个编码盘分成 16 个相等的扇面，每个扇面分别由绝缘体和导体组成，

可表示 0 和 1 两种状态，其中 a、b、c、d 四个位置的扇面组成一组二进制输出，如图 2.11 所示。试问这 16 个二进制数的序列应如何排列，才恰好能组成 0000 到 1111 的 16 组四位二进制输出，同时旋转一周后又返回到 0000 状态？

解：我们发现如果从状态 $a_1a_2a_3a_4$（$a_i=0$ 或 1）逆时针方向旋转一个扇面，那么新的输出是 $a_2a_3a_4a_5$，其中有三位数字不变。因此可以用 8 个结点表示从 000 到 111 这 8 个二进制数。这样从结点（$a_{i-1}\ a_i\ a_{i+1}$）可以到达结点（$a_i\ a_{i+1}$ 0）或（$a_i\ a_{i+1}$ 1），其输出分别为（$a_{i-1}\ a_i\ a_{i+1}$ 0）和（$a_{i-1}\ a_i\ a_{i+1}$ 1）。这样可以得到图 2.12。它是有向连通图，共有 16 条边，且每结点的正、负度相等。由推论 2.3.2，它存在有向欧拉回路。其中任一条都是原问题的解，比如（0000101001101111）就是一种方案。

2.4 哈密顿道路与回路

十九世纪英国数学家哈密顿（Willian Hamilton）给出了关于一个凸 12 面体的数学游戏，他把 12 面体的 20 个顶点比作世界上 20 个城市，30 条棱表示这些城市之间的交通线路。如图 2.13 所示。哈密顿提出能否周游世界，即从某个城市出发，经过每城一次且只一次最后返回出发地。答案是显然的，比如图中的粗线边就表示了其中一种方案。

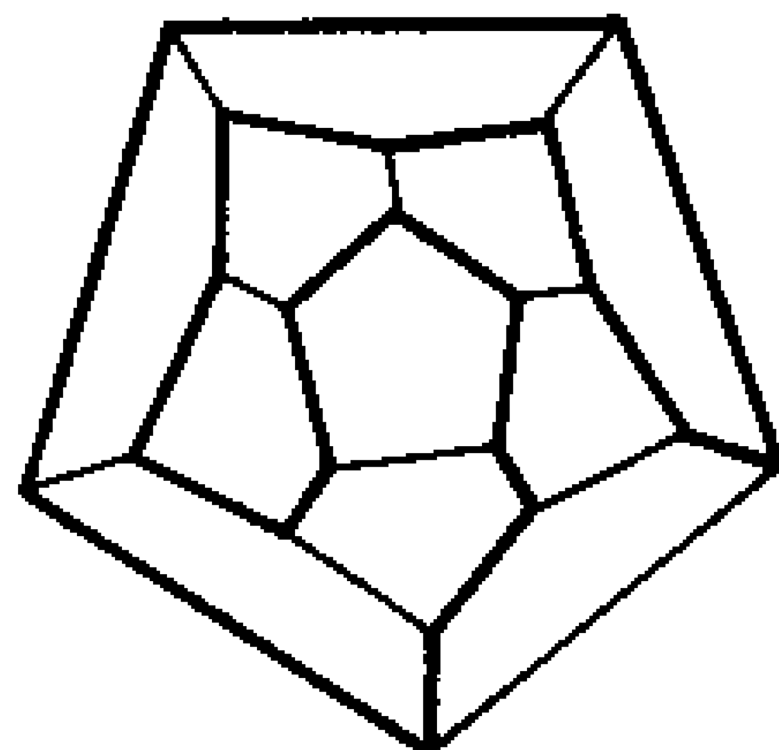


图 2.13

对于任何连通图都可以提出类似问题。

定义 2.4.1 无向图的一条过全部结点的初级回路（道路）称为 G 的哈密顿回路（道路），简记为 H 回路（道路）。

哈密顿回路是初级回路，而不是简单回路，因此它与欧拉回路的概念不同。当然在特殊情况下，G 的一条哈密顿回路恰好也是其欧拉回路。鉴于 H 回路是初级回路，所以如果 G 中含有重边或自环，删去它们之后得到简单图 G'，那么 G 和 G' 关于 H 回路（道路）的存在性是等价的。因此，判定 H 回路存在性问题一般都是针对简单图。

例 2.4.1 完全图 $K_n(n\geqslant 3)$ 中存在 H 回路。

例 2.4.2 图 2.10 的 G 中不存在 H 回路，但存在 H 道路。

有若干存在哈密顿回路（道路）的充分性定理。

定理 2.4.1 如果简单图 G 的任意两结点 v_i，v_j 之间恒有 $d(v_i)+d(v_j)\geqslant n-1$，则 G 中存在哈密顿道路。

证明：先证 G 是连通图。若 G 非连通，则至少分为 2 个连通支 H_1，H_2，其结点数分别为 n_1，n_2。从中各任取一个结点 v_i，v_j，则 $d(v_i)\leqslant n_1-1$，$d(v_j)\leqslant n_2-1$。故 $d(v_i)+d(v_j)<n-1$。矛盾。

以下证 G 存在 H 道路。设 $P=(v_{i_1},v_{i_2},\cdots,v_{i_l})$ 是 G 中一条极长的初级道路，即 v_{i_1} 和 v_{i_l} 的邻点都在 P 上。此时若 $l=n$，P 即为一条 H 道路。若 $l<n$，则可以证明 G 中一定存在经过结点 $v_{i_1},v_{i_2},\cdots,v_{i_l}$ 的初级回路。否则，若边 $(v_{i_1},v_{i_p})\in E(G)$，就不能有 $(v_{i_l},v_{i_{p-1}})\in E(G)$，不然删掉 $(v_{i_p},v_{i_{p-1}})$，就形成了一条过这 l 个结点的初级回路。于是，设 $d(v_{i_l})=k$，

则 $d(v_{i_l}) \leqslant l-k-1$，其中减去 1 表示不能与自身相邻。因此 $d(v_{i_1})+d(v_{i_l})<n-1$。与已知矛盾。所以存在经过 $v_{i_1}, v_{i_2}, \cdots, v_{i_l}$ 的初级回路 C。

由于 G 连通，所以存在 C 之外的结点 v_t 与 C 中的某点 (v_{i_q}) 相邻。删去 $(v_{i_{q-1}}, v_{i_q})$，则 $P'=(v_t, v_{i_q}, \cdots, v_{i_{p-1}}, v_{i_l}, \cdots, v_{i_{q-1}})$ 是 G 中一条比 P 更长的初级道路。以 P' 的两个端点 v_t 和 $v_{i_{q-1}}$ 继续扩充，可得到一条新的极长的初级道路。重复上述过程，因为 G 是有穷图，所以最终得到的初级道路一定包含了 G 的全部结点，即是 H 道路。

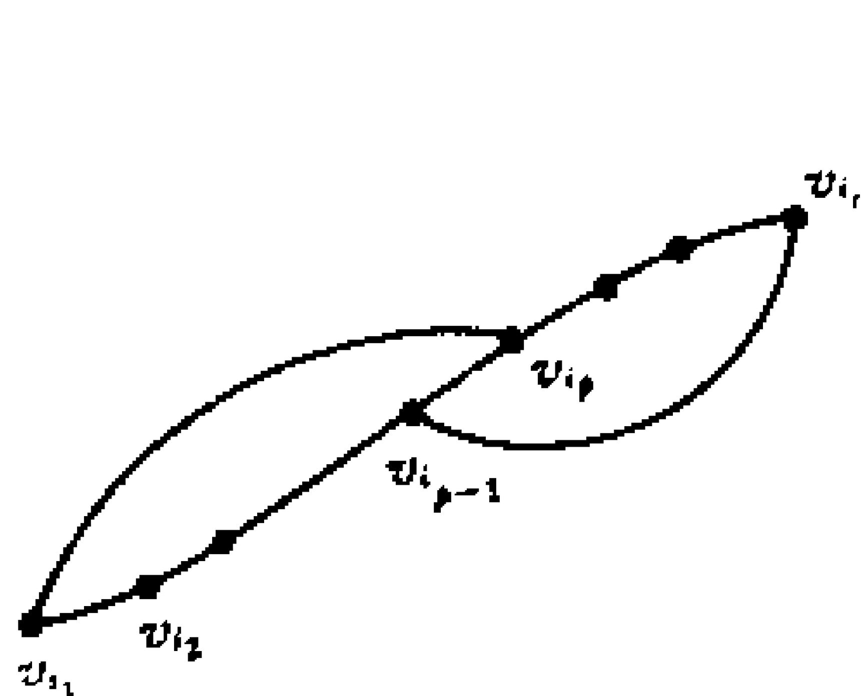


图 2.14

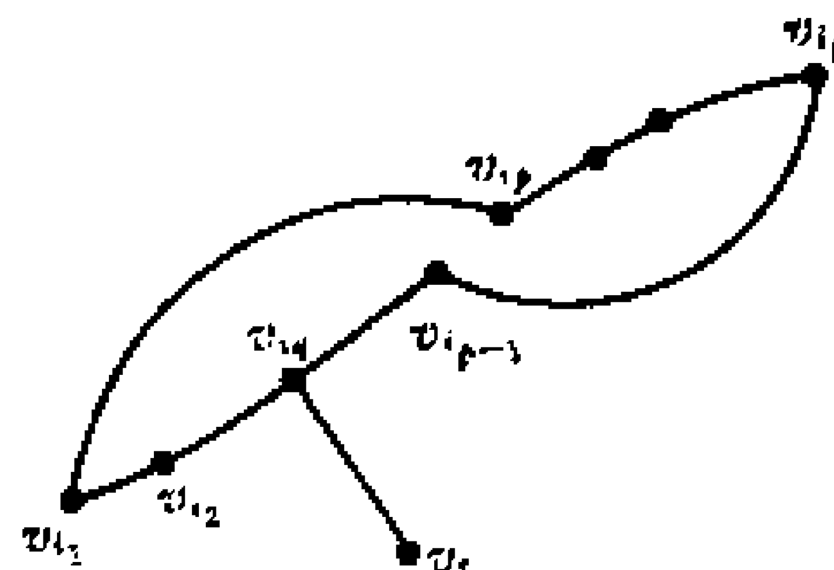


图 2.15

推论 2.4.1 若简单图 G 的任意两结点 v_i 和 v_j 之间恒有 $d(v_i)+d(v_j) \geqslant n$，则 G 中存在哈密顿回路。

证明：由定理 2.4.1，G 有 H 道路。设其两端点是 v_1 和 v_n。若 G 不存在 H 回路，一定有 $d(v_1)+d(v_n) \leqslant n-1<n$，产生矛盾。

推论 2.4.2 若简单图 G 每个结点的度都大于等于 $\frac{n}{2}$，则 G 有 H 回路。

利用推论 2.4.1 即可得出结论。

以下介绍一个更强的 H 回路的存在性定理。

引理 2.4.1 设 G 是简单图，v_i, v_j 是不相邻结点，且满足 $d(v_i)+d(v_j) \geqslant n$。则 G 存在 H 回路的充要条件是 $G+(v_i, v_j)$ 有 H 回路。

证明：必要性显然。现证充分性。假定 G 不存在 H 回路，则 $G+(v_i, v_j)$ 的 H 回路一定经过边 (v_i, v_j)，删去 (v_i, v_j)，即 G 中存在一条以 v_i, v_j 为端点的 H 道路，这时又有 $d(v_i)+d(v_j)<n$。与已知矛盾。

定义 2.4.2 若 v_i 和 v_j 是简单图 G 的不相邻结点，且满足 $d(v_i)+d(v_j) \geqslant n$，则令 $G'=G+(v_i, v_j)$，对 G' 重复上述过程，直至不再有这样的结点对为止。最终得到的图称为 G 的闭合图，记作 $C(G)$。

例 2.4.3 图 2.16(a)的闭合图是(b)。

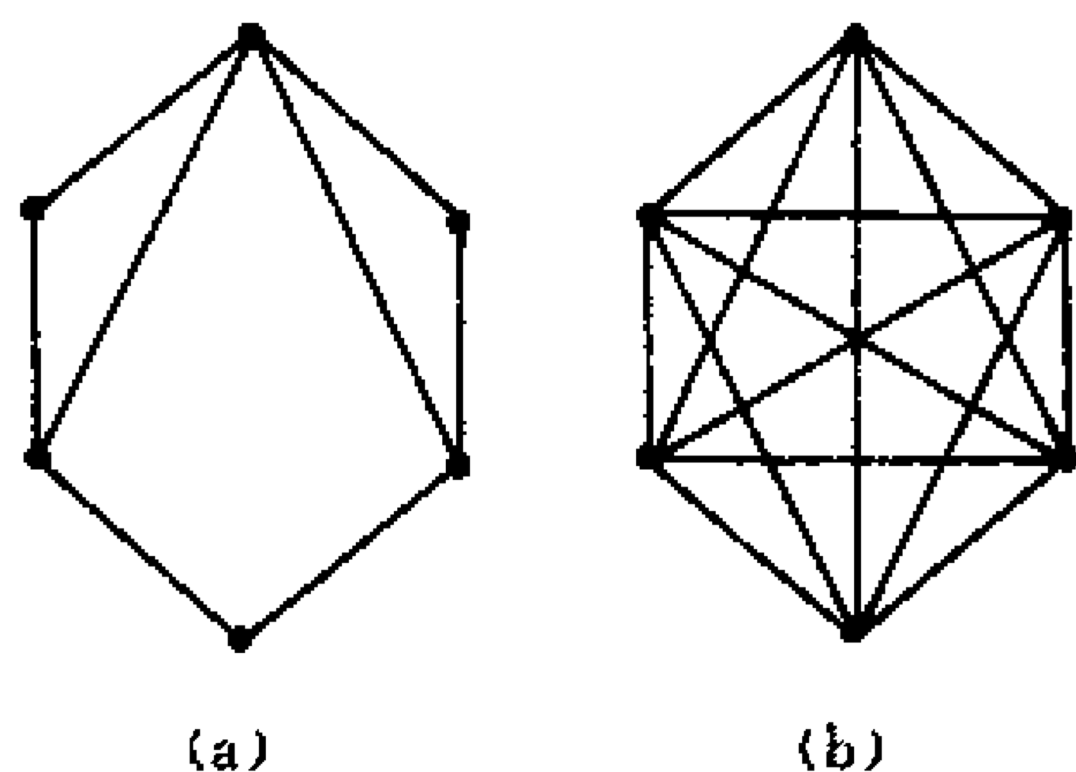


图 2.16

引理 2.4.2 简单图 G 的闭合图 $C(G)$ 是唯一的。

证明：设 $C_1(G)$ 和 $C_2(G)$ 是 G 的两个闭合图，$L_1=\{e_1, e_2, \cdots, e_r\}$，$L_2=\{a_1, a_2, \cdots, a_s\}$ 分别是 $C_1(G)$ 和 $C_2(G)$ 中新加入边的集合，可以证明 $L_1=L_2$，即 $C_1(G)=C_2(G)$。如若不然，不失一般性，设 $e_{i+1}=(u, v) \in L_1$ 是构造 $C_1(G)$ 时

第一条不属于 L_2 的边，亦即 $e_{i+1} \notin C_2(G)$。令 $H=G\cup\{e_1,e_2,\cdots,e_i\}$，这时 H 是 $C_1(G)$ 也是 $C_2(G)$ 的子图。由于构造 $C_1(G)$ 时要加入 e_{i+1}，显然 H 中满足 $d(u)+d(v)\geqslant n$，但 $(u,v)\notin C_2(G)$，与 $C_2(G)$ 是 G 的闭合图矛盾。

定理 2.4.2 简单图 G 存在哈密顿回路的充要条件是其闭合图存在哈密顿回路。

证明：设 $C(G)=G\cup L_1$，$L_1=\{e_1,e_2,\cdots,e_t\}$，由引理 2.4.1 和 2.4.2，$G$ 有 H 回路 $\Leftrightarrow$ $G+e_1$ 有 H 回路 $\Leftrightarrow\cdots\Leftrightarrow G\cup L_1$ 有 H 回路。由于 $C(G)$ 唯一，故定理得证。

推论 2.4.1 和 2.4.2 都是定理 2.4.2 的自然结果。

推论 2.4.3 设 $G(n\geqslant3)$ 是简单图，若 $C(G)$ 是完全图，则 G 有 H 回路。

例 2.4.4 图 2.16(a)有 H 回路。

例 2.4.5 设 $n(\geqslant3)$ 个人中，任两个人合在一起都认识其余 $n-2$ 个人。证明这 n 个人可以排成一队，使相邻者都互相认识。

证明：每个人用一个结点表示，相互认识则用边连接相应的结点，于是得到简单图 G。若 G 中有 H 道路，则问题得证。由已知条件，对任意两点 $v_i,v_j\in V(G)$，都有 $d(v_i)+d(v_j)\geqslant n-2$。此时若 v_i 与 v_j 相识，即 $(v_i,v_j)\in E(G)$，则 $d(v_i)+d(v_j)\geqslant n$；若不相识，必存在 $v_k\in V(G)$，满足 $(v_i,v_k),(v_j,v_k)\in E(G)$。否则，设 $(v_i,v_k)\notin E(G)$，就出现 v_k,v_j 合在一起不认识 v_i，与原设矛盾。因此也有 $d(v_i)+d(v_j)\geqslant n-1$。综上由定理 2.4.1，$G$ 中存在 H 道路。

例 2.4.6 证明图 2.17 中没有 H 回路。

证明：H 回路是经过每个结点一次的初级回路。经观察，如果给某个结点标以 A，它的邻接点标以 B，B 的邻接点再标以 A，则可顺利标完 G 的全部结点。若 G 中有 H 回路，该回路一定是沿 $ABAB\cdots AB$ 走完全部结点，即标 A 与标 B 的结点数相同，由于 $|V(G)|$ 是奇数，因此 G 中没有 H 回路。

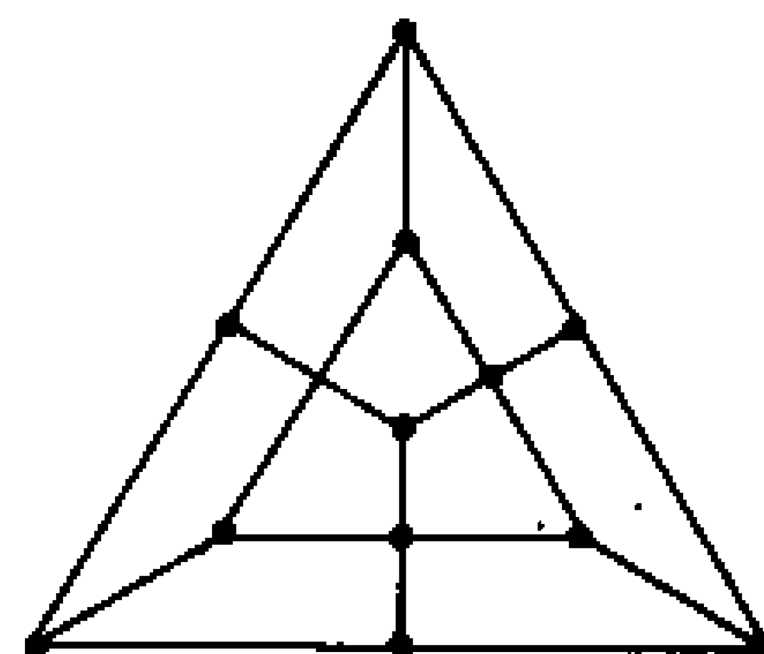


图 2.17

例 2.4.7 地图不存在相交的边界。如果一个地图中有 H 回路，则可以用 4 种不同颜色对它们的域进行着色，使相邻的域染不同的颜色。

证明：我们用一个示意图加以直观的说明。设 H（粗线边）是 G 中的一个哈密顿回路，则 H 将 G 的域划分成回路内外两部分。每一部分的域用 2 种颜色可以染色，满足相邻域染不同颜色。不然，一定存在三个以上的域互相邻接的情形。此时必出现 v' 这样的结点。这与 H 是哈密顿回路相悖。因此结论正确。

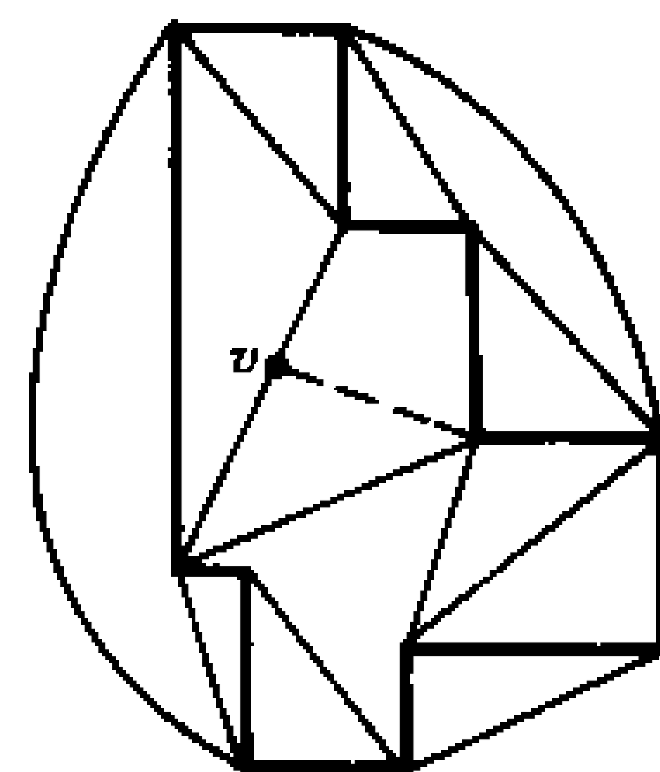


图 2.18

一般情况下，给定一个图 G，判定它是否存在 H 回路，需要使用搜索法。首先去掉重边和自环，然后采用 DFS 等算法是可以实现的。但是在最坏情况下其计算复杂度与 $n!$ 成正比，它是属于 NP(Nondeterministic Polynomial)完全问题。

2.5 旅行商问题

上节讨论的哈密顿回路不涉及边的长度。但是在许多实际问题中，每条边都可以有它的权。边权可以是该路的长度，旅行的费用或所需的时间。这样需要在可能众多的 H 回路中挑选总长最短(或总化费最省，旅途时间最少)的一条。显然这种问题的求解难度也非常大。

给定一个正权完全图，求其总长最短的哈密顿回路，这就是著名的旅行商问题。容易知道，对 n 个结点的完全图，存在 $\frac{1}{2}(n-1)!$ 个不同的 H 回路。旅行商问题也属于 NP 完全问题。如果采用枚举法，将需要对 $\frac{1}{2}(n-1)!$ 个不同的 H 回路进行比较，在 n 较大时，这在计算上是不可行的。对这类问题一种好的精确求解法是分支与界法。以下我们举例说明它的基本思路。

例 2.5.1 图 2.19 表示 5 个城市间的铁路线，各边的值表示该线路的旅途费用。求从 v_1 出发经各城市一次且仅一次最后返回 v_1 总费用最省的一条路径。

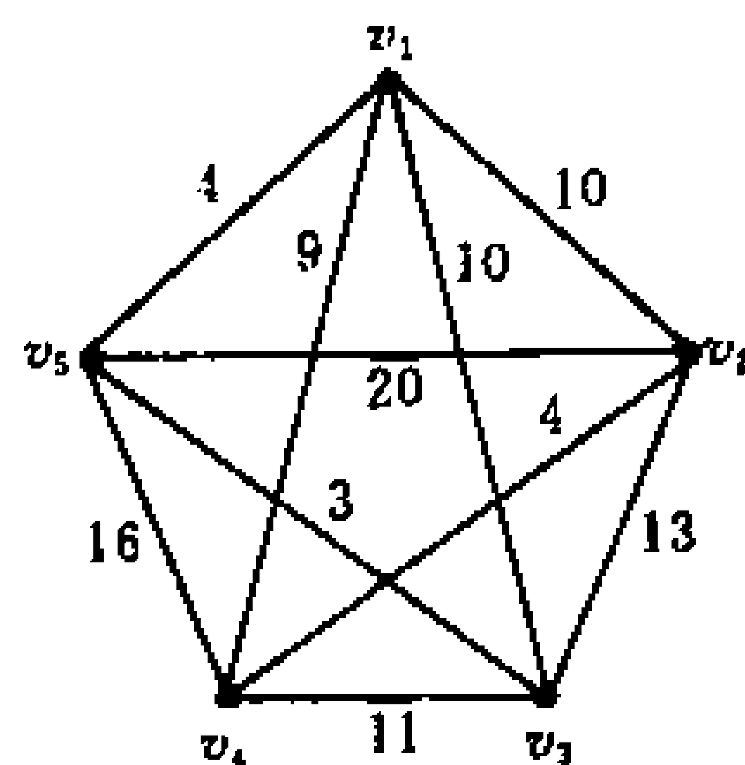


图 2.19

解：该问题就是求 G 的一条最短的 H 回路。采用分支与界法的基本思路是：

1. 首先将边权由小至大排序，初始界 $d_0 \leftarrow \infty$。该例中

a_{ij}:	a_{53}	a_{42}	a_{15}	a_{14}	a_{12}	a_{13}	a_{34}	a_{23}	a_{45}	a_{25}
l_{ij}:	3	4	4	9	10	10	11	13	16	20

为了尽快找到最优解，我们采用 DFS 方法和以下的分支判断步骤：

2. 在边权序列中依次选边进行深探，直至选取 n 条边，判断是否构成 H 回路(每个结点标号只出现 2 次，且这些边只构成一个回路)，若是，$d_0 \leftarrow d(s_1)$，结束。

该例中

$d(s_1)=d(1)=d(a_{53},a_{42},a_{15},a_{14},a_{12})=30$。

由于 v_1 出现了 3 次，故非所求。

3.(继续深探) 依次删除当前 s_i 中的最长边，加入后面第一条待选边，进行深探，如果它是 H 回路且 $d(s_i)<d_0$，则 $d_0 \leftarrow d(s_i)$ 作为界。

4.(退栈过程) 不能再深探时需要退栈。如果栈空，结束，其最佳值为 d_0。否则如果新分支的 $d(s_i)\geqslant d_0$，继续退栈；若 $d(s_i)<d_0$，转 3。

整个求解过程如图 2.20 所示，其中 $\bar{a}_{ij}$ 表示删除 a_{ij}，a_{ij} 表示保留该边。由于 $d(6)=32$，是合理解，同时其余分支的值都大于它，因此它是最短的 H 回路。

图 2.20 中

$d(1)=d(a_{53},a_{42},a_{15},a_{14},a_{12})=30$。

$d(2)=d(a_{53},a_{42},a_{15},a_{14},a_{13})=30$。

$d(3)=d(a_{53},a_{42},a_{15},a_{14},a_{34})=31$。

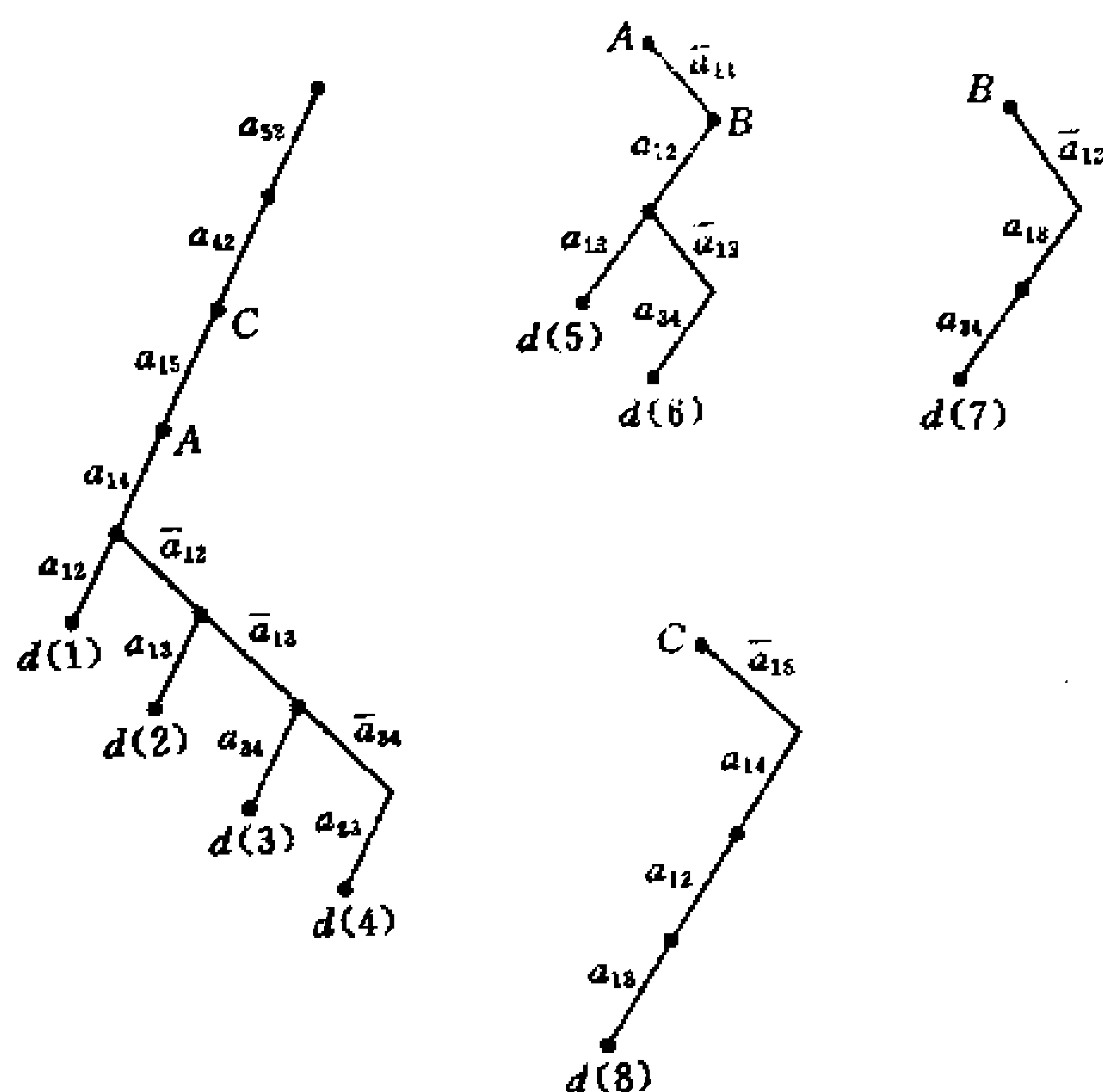


图 2.20

$d(4)=d(a_{53},a_{42},a_{15},a_{14},a_{23})=33$ *。

$d(5)=d(a_{53},a_{42},a_{15},a_{12},a_{13})=31$。

$d(6)=d(a_{53},a_{42},a_{15},a_{12},a_{34})=32$ *。

$d(7)=d(a_{53},a_{42},a_{15},a_{13},a_{34})=32$。

$d(8)=d(a_{53},a_{42},a_{14},a_{12},a_{13})=36$。

所以最优解为 $d(6)=32$。

由于对边权进行了排序，因此每删去一条短边，增一条长边，其总和是非减的。即该结点以下分支的各种状态的值都不会小于该点的值。同时由于一切合理的与不合理的解都大于等于 d_0，因此 d_0 必为最优解。

从以上分析看，这种搜索过程是在不断地构造分支与确定界值。一旦确定了界值，则对大于等于界值的分支不再搜索，而且最后得到的界值就是问题的最佳解。因此这种方法称为分支与界法。从该例看，分支与界法比枚举法优越得多，但是在最坏情况下，其计算复杂度仍为 $O(n!)$。因此在实际问题中，人们经常采用近似算法求得问题的近似最优解，从而避免浩翰的计算量。

在设计近似算法时，往往需要对原问题增加一些限制，以便能够提高计算速度和近似效果。而这些限制又常常都是比较符合实际的。比如旅行商问题里的限制是：(1)G 是无向正权图。(2)符合三角不等式，即任意结点 v_i,v_j 和 v_k 之间，两边长度之和大于等于第三边长度。在这些条件下，旅行商问题有多种近似算法。这里我们介绍"便宜"算法。

算法描述如下：

a. 置 $\bar{S}=\{2,3,\cdots,n\}$，$w(1,1)\leftarrow 0$，$k\leftarrow 1$，序列 $T=(1,1)$，

$w(i,k)=w(i,1)$，$i\in\bar{S}$。

b. 在 $\bar{S}$ 中，令

$w(j,t)=\min\limits_{\substack{i\in\bar{S}\\k\in T}} w(i,k)$,

对回路 T 中的边 (t,t_1)，(t,t_2)，

若 $w(j,t_1)-w(t,t_1)\leqslant w(j,t_2)-w(t,t_2)$，

则 j 插入到 T 的 t,t_1 之间，否则 j 插入到 T 的 t,t_2 之间，

$\bar{S}\leftarrow\bar{S}-j$，

若 $\bar{S}=\Phi$，结束。否则转 c。

c. 对全部 $i\in\bar{S}$，置

$w(i,k)\leftarrow\min(w(i,k),w(i,j))$，

转 b。

算法中，T 是一个不断扩充的初级回路，最初是一个自环。在步骤 b 中，首先选取 $\bar{S}$ 中与 T 距离最近的一个结点 j。设 (j,t) 是相应的边。这时结点 j 或插入到回路 T 中 t 的前面，或插到其后。这根据 j 插入后回路 T 长度增量的大小而定。即如果 $w(j,t)+w(j,t_1)-w(t,t_1)\leqslant w(j,t)+w(j,t_2)-w(t,t_2)$，则插入到 t 与 t_1 之间。否则在 t 与 t_2 之间。这就是"便宜"的含义。

例 2.5.2 已知图 G 的权矩阵，其旅行商问题采用便宜算法近似求解的过程如图 2.21所示。

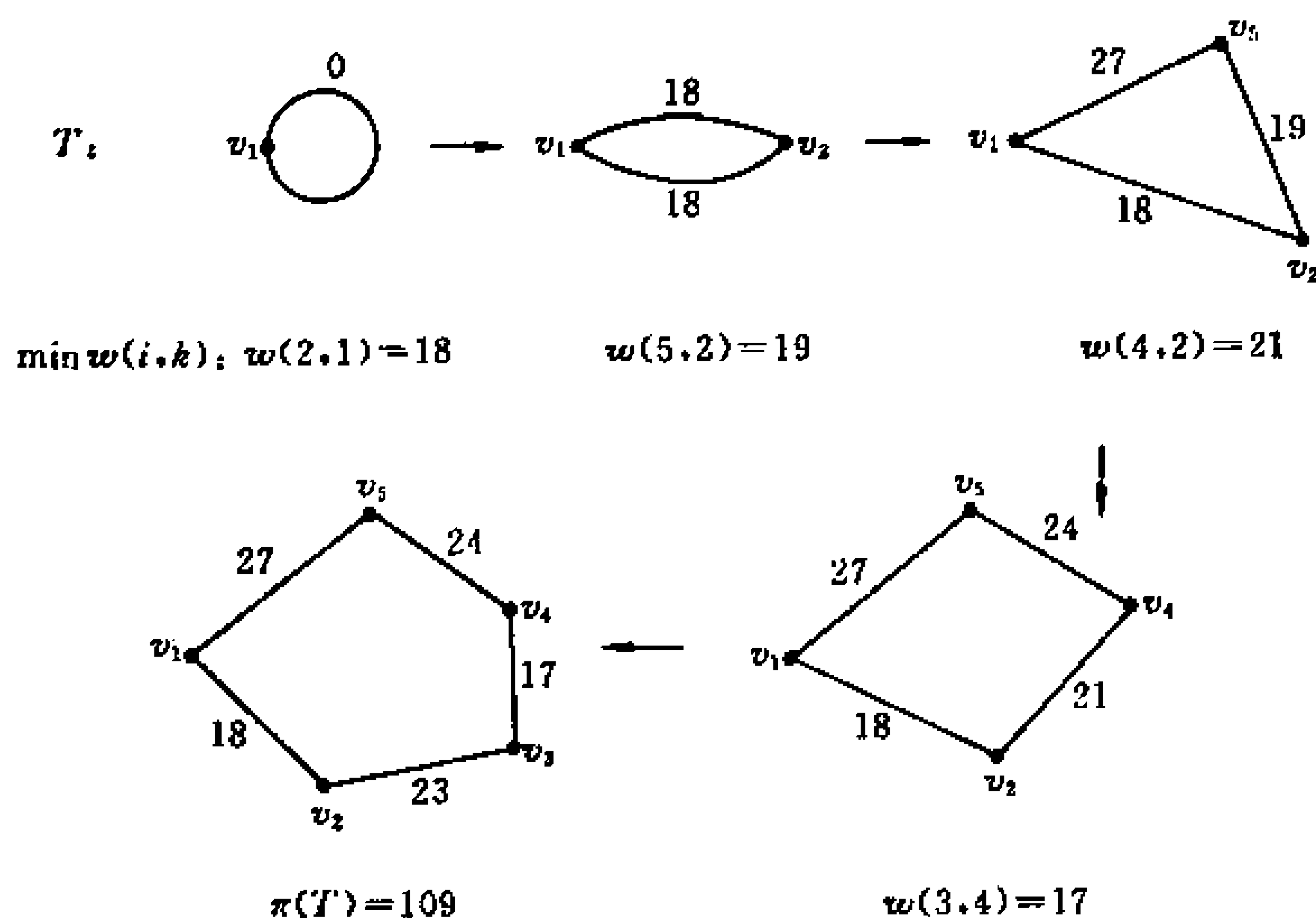


图 2.21

$$\begin{bmatrix} 0 & 18 & 35 & 25 & 27 \\ 18 & 0 & 23 & 21 & 19 \\ 35 & 23 & 0 & 17 & 28 \\ 25 & 21 & 17 & 0 & 24 \\ 27 & 19 & 28 & 24 & 0 \end{bmatrix}$$

定理 2.5.1 设正权完全图的边权满足三角不等式，其旅行商问题的最佳解是 O_n，使

宜算法的解是 T_n。则$\frac{T_n}{O_n}<2$。

证明：设往初级回路 T 中每加入一个结点 j 后，该回路的增量是 δ_j，$\delta_j=w_{jt}+w_{jt'}-w_{tt'}$。我们将证明 δ_j 与最佳解中除最长边之外的某条边（设长度为 lu）形成对应，并且 $\delta_j\leqslant 2lu$。

初始 $T_0=0$，当加入一个结点 j 后，由于 $w(j,1)=\min\limits_{i\in S}w(i,1)$，当然 $w(j,1)$不会大于 O_n 中结点 1 所关联的两条边中任意一个边权。取其中小的边权为 lu，自然有 $\delta_j\leqslant 2lu$。在 G 中删去权为 lu 的边，即构成对应。

设 T_{n-1}时满足条件，则构造 T_n 时，O_n 中肯定有一些尚未删除的边与 T_{n-1}中的结点关联，否则与 O_n 是 H 回路矛盾。设其中最短边是(p,q)，如图 2.22 所示。假定此时由算法加入 T_n 的边不是(p,q)，而是(j,t)。显然

$$w(j,t)\leqslant w(p,q)。\tag{1}$$

由不等式

$$w(j,t_i)\leqslant w(j,t)+w(t,t_i),\ i=1,2,$$

$$\therefore\quad w(j,t_i)\leqslant w(p,q)+w(t,t_i)。\tag{2}$$

由(1)(2)式立得

$$\delta_j\leqslant 2w(p,q)。$$

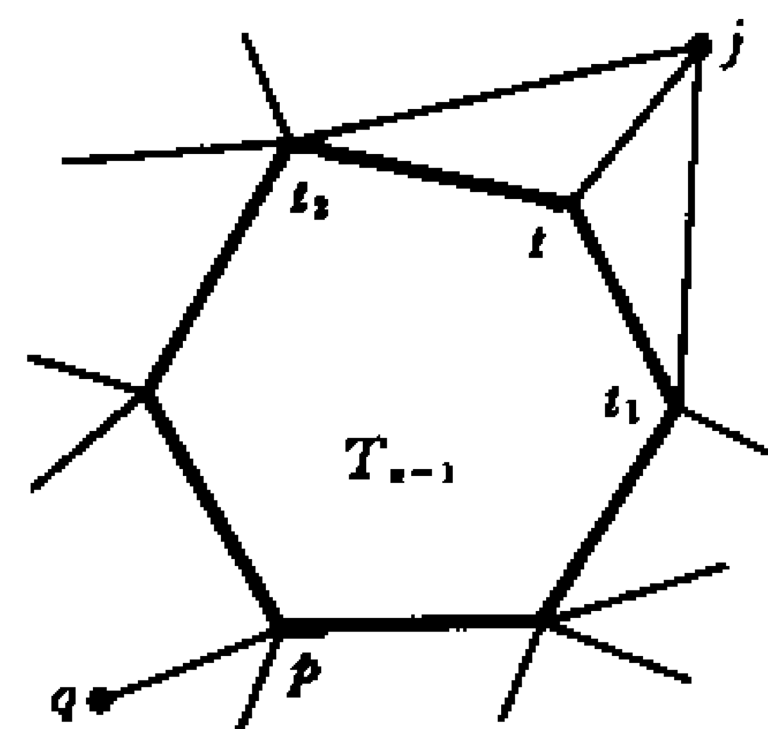


图 2.22

此时 δ_j 与 O_n 中的边(p,q)对应，删除(p,q)。因此 T_n 时也满足条件。定理得证。

便宜算法的计算复杂度是 $O(n^2)$。其效率比枚举法或分支与界法要高得多。虽然从理论上讲它的近似程度并非理想，但是在实际上它与最优解常常十分接近。比如例 2.5.2 的最优解是 107，而便宜算法的解是 109。

2.6 最短路径

以下三节讨论赋权图的最优化道路。它们都具有明显的实际背景，有相当重要的应用价值。

按照实际问题的模型，最短路径问题可以包括：

1. 某两结点之间的最短路径。
2. 某结点到其它各结点的最短路径。
3. 任意两结点之间的最短路径。

相应地图 G 各边的权 $w(e)$还可以有如下特点：(a)均大于 0；(b)均等于 1；(c)是任意实数。容易看出，如果模型 2 得到解决，模型 1 和模型 3 就能迎刃而解。因此我们将只依边权的三种情形讨论模型 2 的最短路径，并且局限于求 v_1 到其它各点的最短路径。

v_1 到 v_i 的一条路径 $P(i)$的长度记为 $\pi(i)$。

$$\pi(i)=\sum_{e\in P(i)}w(e)。$$

$w(e)$表示边 $e=(v_j,v_k)$的权，也记为 w_{jk}。结点 v_1 到 v_i 的最短路径就是满足上式的极小的 $\pi(i)$。

如果一条长度为$\pi(i)$的道路$P(i)$中包含有回路C，令$P'(i)$是其中不含C的初级道路，显然$\pi(i)=\pi'(i)+\pi(C)$。其中$\pi(C)$表示回路C的长度。若$\pi(C)<0$，即C是负长回路，则v_1到v_i不可能有最短路径；若$\pi(C)\geqslant 0$，则$\pi'(i)\leqslant\pi(i)$，即v_1到v_i的最短路径一定是初级道路。本节讨论的都是无负长回路的图。

2.6.1 正权图中v_1到各点的最短路径

引理 2.6.1 正权图G中，如果$P(i)$是v_1到v_i的最短路，且$v_j\in P(i)$，则$P(j)$是v_1到v_j的一条最短路。

证明：如果$P(j)$不是最短路，则存在一条最短路$P'(j)$，使$\pi'(j)<\pi(j)$，这样$\pi'(i)=\pi'(j)+\pi(j,i)<\pi(i)=\pi(j)+\pi(j,i)$，与$P(i)$是最短路矛盾。

引理 2.6.2 正权图中任意一条最短路径的长度大于其局部路径长度。

结论是显然的。

假定已经知道从v_1到其余各点的最短路$P(i_k)(k=1,2,\cdots,n)$，并且满足

$$\pi(1)=\pi(i_1)\leqslant\pi(i_2)\leqslant\cdots\leqslant\pi(i_n)。$$

由引理 2.6.2 知，若$k>l(l\geqslant 1)$，则$P(i_k)$不可能是$P(i_l)$的一部分。再由引理 2.6.1 可得

$$\pi(i_l)=\min_{1\leqslant j<l}\pi(i_j)+W_{i_j,i_l}。$$

这就是最短路径的 Dijkstra 算法的基础。

Dijkstra 算法描述如下：

a. 置$\bar{S}=\{2,3,\cdots,n\}$，$\pi(1)=0,\pi(i)=\begin{cases}w_{1i} & i\in\Gamma_1^+\\ \infty & 其它\end{cases}$

b. 在$\bar{S}$中，令

$$\pi(j)=\min_{i\in\bar{S}}\pi(i)，$$

置$\bar{S}\leftarrow\bar{S}-\{j\}$，

若$\bar{S}=\Phi$，结束。否则转 c。

c. 对全部$i\in\bar{S}\cap\Gamma_j^+$，置

$$\pi(i)\leftarrow\min(\pi(i),\ \pi(j)+w_{ji})，$$

转 b。

其中执行步骤 c 时，j已属于$S(V(G)-\bar{S})$，因此$\bar{S}$中可能使$\pi(i)$发生变化的只能是j的直接后继。

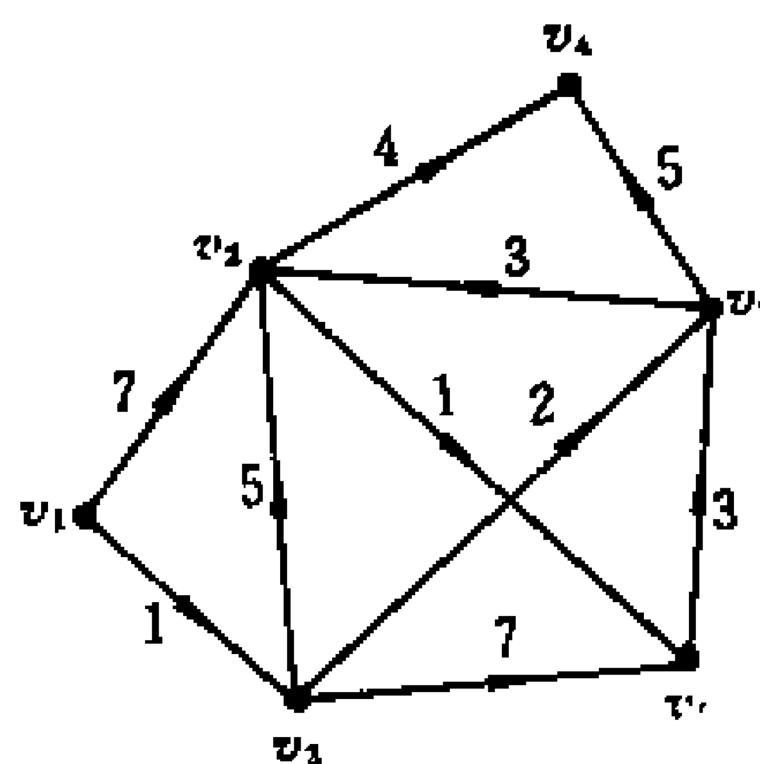


图 2.23

例 2.6.1 用 Dijkstra 算法求图 2.23 中v_1到其余各点的最短路过程如下：

1. $\pi(3)=\min\pi(i)=1$,
   $\pi(2)=6,\pi(4)=\infty$,
   $\pi(5)=3,\pi(6)=8$,
2. $\pi(5)=\min\pi(i)=3$,
   $\pi(2)=6,\pi(4)=8,\pi(6)=8$,
3. $\pi(2)=\min\pi(i)=6$,
   $\pi(4)=8,\pi(6)=7$,

4. $\pi(6)=\min\pi(i)=7$,

  $\pi(4)=8$,

5. $\pi(4)=\min\pi(i)=8$。

为了得到具体的路径走向，可以增设一个 n 维向量 Q，初值均为 1；然后将步骤 c 改为：

c. 对全部 $i\in\bar{S}\cap\Gamma_j^+$

  若 $\pi(i)>\pi(j)+w_{ji}$,

  则 $\pi(i)\leftarrow\pi(j)+w_{ji}$, $Q(i)\leftarrow j$,

  转 b。

这样，$Q(i)$ 中存放的是最短路 $P(i)$ 中 v_i 的直接前趋的结点号。比如上例运算结束时 Q 中的值是

1	5	1	5	3	2

例如从中可查，$Q(6)=v_2$，$Q(2)=v_5$，$Q(5)=v_3$，$Q(3)=v_1$，因此最后可以得到 v_1 到 v_6 的最短道路是 (v_1,v_3,v_5,v_2,v_6)。

Dijkstra 算法的正确性前面已经论述，以下讨论其计算复杂度。

算法的基本步骤是 b 和 c。b 所需要的比较次数取决于所采用的数据结构。如果 $\bar{S}$ 使用特征向量 Φ 存储，使

$$\Phi(i)=\begin{cases}1, & 若\ i\in\bar{S}。\\ 0, & 其它。\end{cases}$$

那么在 b 的迭代需要 $|\bar{S}|$ 次比较，总比较次数是 $\frac{1}{2}n(n-1)$。

如果采用邻接表的形式表示图 G，由于每个结点的直接后继顺序可查，那么步骤 c 最多需要 $m(=\sum_j d_j^+)$ 次加法和比较。这样 Dijkstra 算法的计算复杂性是 $O(m)+O(n^2)$。

2.6.2 边权为 1 时 v_1 到各点的最短路

在有些情况下，图 G 所有的边权都相同。这时可以对 Dijkstra 算法进行改进，从而计算 v_1 到其余各点的最短路径。

算法描述如下：

a. 置 $\pi(1)=0$，$\pi(i)=\infty$，$i\geqslant 2$，

  $k=0$，$S=\{1\}$，$S_0=\{1\}$。

b. 第 k 步

  置 $S_{k+1}=\Gamma_{S_k}^+\cap\bar{S}$，

  $\pi(i)=k+1$，$i\in S_{k+1}$，

  $S=S\cup S_{k+1}$。

c. 若 $|S|=|V(G)|$，结束；否则 $k\leftarrow k+1$，转 b。

当算法进行第 k 次迭代时，已经有 $S_k=\{i\mid\pi(i)=k\}$ 以及 $S=\{i\mid\pi(i)\leqslant k\}$。此外 $\Gamma_{S_k}^+$ 表示结点集 S_k 中所有结点的直接后继集合。

例 2.6.2 使用本算法求图 2.24 中 v_1 到其余各点的最短路径过程如下：

a. $\pi(1)=0, \pi(i)=\infty$,

$i=2,3,4,5,6, s=\{1\}$,

b. $k=0, s_0=\{1\}, s_1=\{2,3\}$,

$\pi(2)=\pi(3)=1, s=\{1,2,3\}$,

c. $k=1, s_2=\{4,5,6\}$,

$\pi(4)=\pi(5)=\pi(6)=2, S=V(G)$。

d. end。

定理 2.6.1 如果图 G 是以正向表或邻接表的数据结构表示，则本算法的计算复杂性是 $O(m)$。

2.6.3 边权任意时 v_1 到各点的最短路

当存在负权边时，情况会变得复杂一些。对一条权为 w_{ij} 的边 (v_i, v_j) 来说，因为从 v_1 到 v_j 的最短路可能经过 v_i，假定 $w_{ij}<0$，在 $G-e_{ij}$ 中很可能 $\pi(j)<\pi(i)$，例如在某个图 G 中 $w_{ij}=-2$，而 $G-e_{ij}$ 有 $\pi(i)=8, \pi(j)=7$，就符合这种情况。如果仍然采用 Dijkstra 算法，则 $\pi(j)$ 至少为 7，而不是最多为 6。因此，在有负权边时，Dijkstra 算法可能失效。

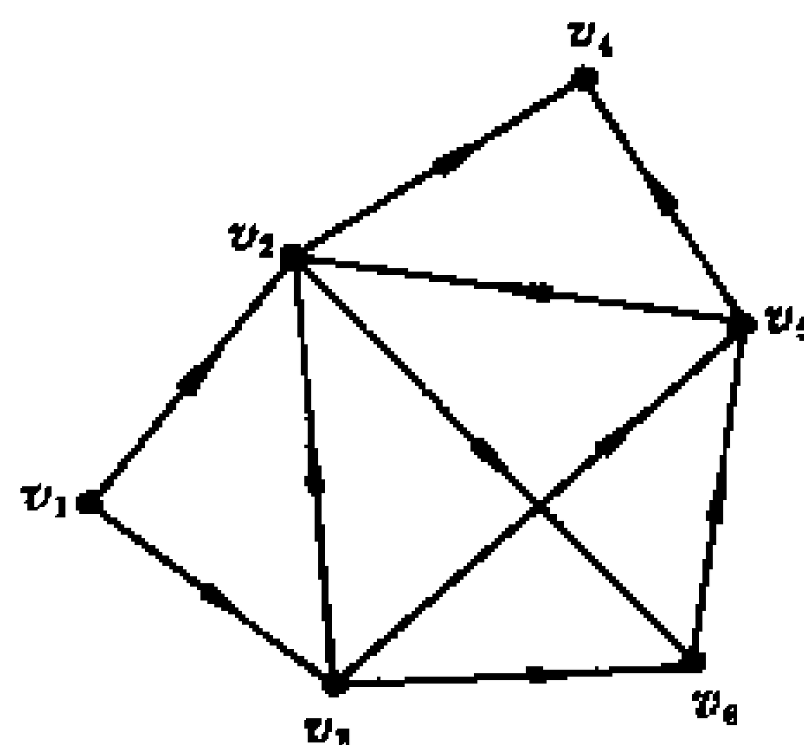


图 2.24

Ford 给出的算法解决了这一问题，现描述如下。

a. 置 $\pi(1)=0, \pi(i)=\infty$,　　　$i=2,3,\cdots,n$,

b. i 从 2 到 n，令

$$\pi(i) \leftarrow \min[\pi(i), \min_{j\in\Gamma_i^-}(\pi(j)+w_{ji})],$$

c. 若全部 $\pi(i)$ 都没变化，结束；否则转 b。

在算法的每一步，$\pi(i)$ 都是从 v_1 到 v_i 的最短路径长度的上界。由于不存在负长回路，因此 v_1 到 v_i 的最短路长度是 $\pi(i)$ 的下界。

由于 $\pi(i)$ 在减小而且有下界，所以算法收敛同时存在极限。以下证明该极值确是从 v_1 到 v_i 的最短路长度。设算法结束时，对某个结点 v_s 有 $\pi(s)$，假定它经过的路径是 $(1, s_k, s_{k-1}, \cdots, s_2, s_1, s)$，显然有

$$\pi(s)=w(1,s_k)+w(s_k,s_{k-1})+\cdots+w(s_1,s),$$

对从 v_1 到 v_s 的另一条路径，比如 $\mu=(1,t_h,t_{h-1},\cdots,t_1,s)$，由于步骤 b 的等式成立，所以有

$$\pi(s)-\pi(t_1)\leqslant w(t_1,s),$$

$$\pi(t_1)-\pi(t_2)\leqslant w(t_2,t_1),$$

$$\cdots\cdots$$

$$\pi(t_h)-\pi(1)\leqslant w(1,t_h),$$

即 $\pi(s)\leqslant w(\mu)=w(1,t_h)+w(t_h,t_{h-1})+\cdots+w(t_1,s)$。

因此 $\pi(s)$ 是从 v_1 到 v_s 的最短路长。算法的正确性得证。以下讨论计算复杂性。

如果采用逆向表结构，步骤 b 需要进行 m 次加法和比较，现在分析 c，即 b 要迭代的

次数。假定没有负回路，则从 v_1 到任何其它结点的最短路径不会超过 $n-1$ 条边，因此经过 $n-1$ 次迭代之后 $\pi(i)$将保持不变。当然如果在第 n 次迭代时它仍在发生变化，只能说明存在负长回路。因此有

定理 2.6.2 在最坏情况下 Ford 算法的计算复杂性是 $O(mn)$。

例 2.6.3 使用 Ford 算法求图 2.25 中 v_1 到其它各点最短路的过程如下：

a. $\pi(1)=0$，$\pi(2)=\pi(3)=\pi(4)=\pi(5)=\pi(6)=\infty$。

b. $\pi(2)=7$，$\pi(3)=8$，$\pi(4)=11$，$\pi(5)=8$，$\pi(6)=9$。

c. $\pi(2)=7$，$\pi(3)=6$，$\pi(4)=10$，$\pi(5)=8$，$\pi(6)=8$。

d. $\pi(2)=7$，$\pi(3)=6$，$\pi(4)=10$，$\pi(5)=8$，$\pi(6)=8$。

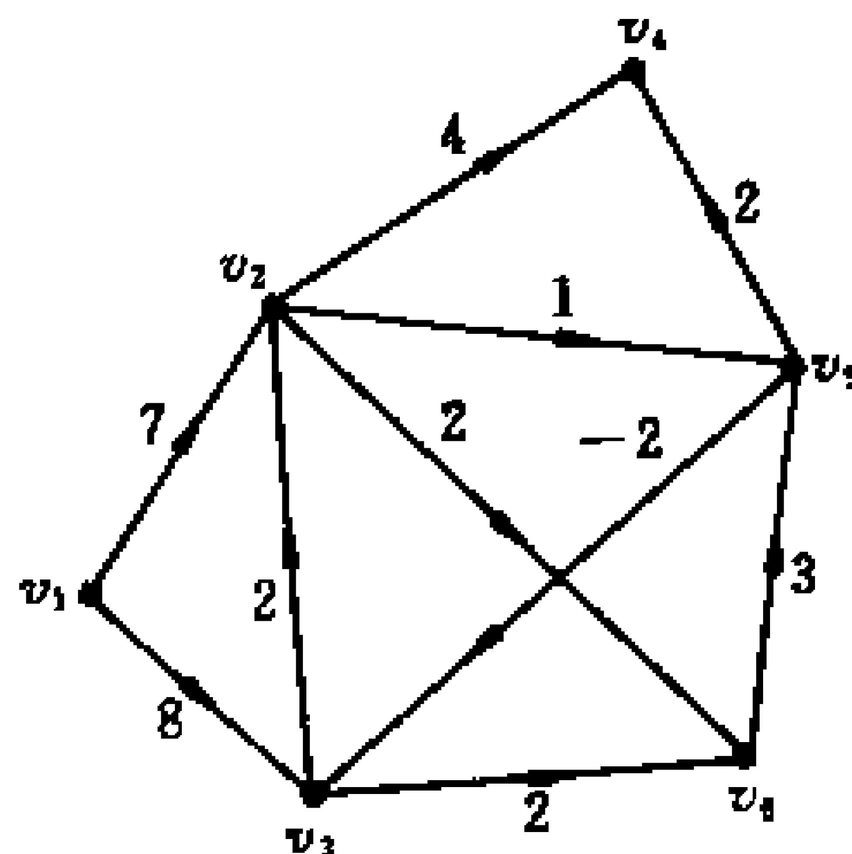


图 2.26

由于 Ford 算法主要取决于步骤 b 的迭代次数，因此 G 中结点被检查的次序对算法收敛的快慢显得很重要。比如，若 G 中负权边数很少时，可以先忽略（相当于删除）它们而采用 Dijkstra 算法，这样可以得到一个结点序，并把从 v_1 到各点的无负权边时的最短路长度作为上界。用它取代步骤 a，就能有效地提高算法的效率。

例 2.6.4 对图 2.25 采用这样改进后的运算结果是：

a. $\pi(1)=0$，$\pi(2)=7$，$\pi(3)=8$，$\pi(4)=10$，$\pi(5)=8$，$\pi(6)=9$，

因此结点序是(1,2,3,5,6,4)。

b. $\pi(2)=7$，$\pi(3)=6$，$\pi(5)=8$，$\pi(6)=8$，$\pi(4)=10$。

b. $\pi(2)=7$，$\pi(3)=6$，$\pi(5)=8$，$\pi(6)=8$，$\pi(4)=10$。

2.7 关键路径

一项工程任务，大到建造一座水坝、一枚航天火箭，一座体育中心，小至组装一台机床，一架电视机，都要包括许多工序。这些工序相互约束，只有在某些工序完成之后，一个工序才能开始。即它们之间存在完成的先后次序关系，一般认为这些关系是预知的，而且也能够预计完成每个工序所需要的时间。这时工程领导人员迫切希望了解最少需要多少时间才能够完成整个工程项目，影响工程进度的要害工序是哪几个？

本节我们只研究其中的一种特例，即工序之间只存在时间次序的约束，也就是说如果某工序 i 尚未完成，工序 j 就不能启动。这样，工程可以被分解为一些基本工序，工序 i 所需时间用 w_i 表示，工序之间的约束情况可以用边来表示。这样可以得到两种类型的图。

2.7.1 PT 图

在 PT(Potentialtask graph)图中，用结点表示工序，如果工序 i 完成之后工序 j 才能启动，则图中有一条有向边(i,j)，其长度 w_i 表示工序 i 所需的时间。

例 2.7.1 建造一座楼房底层的工序共有 10 个，如表 2.7.1 所示。各工序所需的时间是确定的。

表 2.7.1

序　号	名　称	所需时间(天)	先序工序
1	基础设施	15	
2	下部砌砖	5	1
3	电线安装	4	1
4	圈梁支模	3	2
5	水暖管道	4	2
6	大梁安装	2	4,5
7	楼板吊装	2	6,9,10
8	楼板浇模	3	6,9,10
9	吊装楼梯	3	4,5
10	上部砌砖	4	2

相应的 PT 图是图 2.26。图中 v_i 表示作业 i，以 v_i 为始点的边权是作业 v_i 的时间。作业 v_i 最早开始时间应在以 v_i 为终点的作业完成之后。例如作业 v_4 只能在 20 时刻才能开始，23 时刻才能完成，而作业 v_5 需 24 时刻才能完成，因此作业 v_6 最早只能在 24 时刻才能开始。因此，作业 v_i 的最早开始时间恰是 v_1 到 v_i 的最长路径长度，整个工程的最早完工时间是 v_1 到 v_n 的最长路长度。

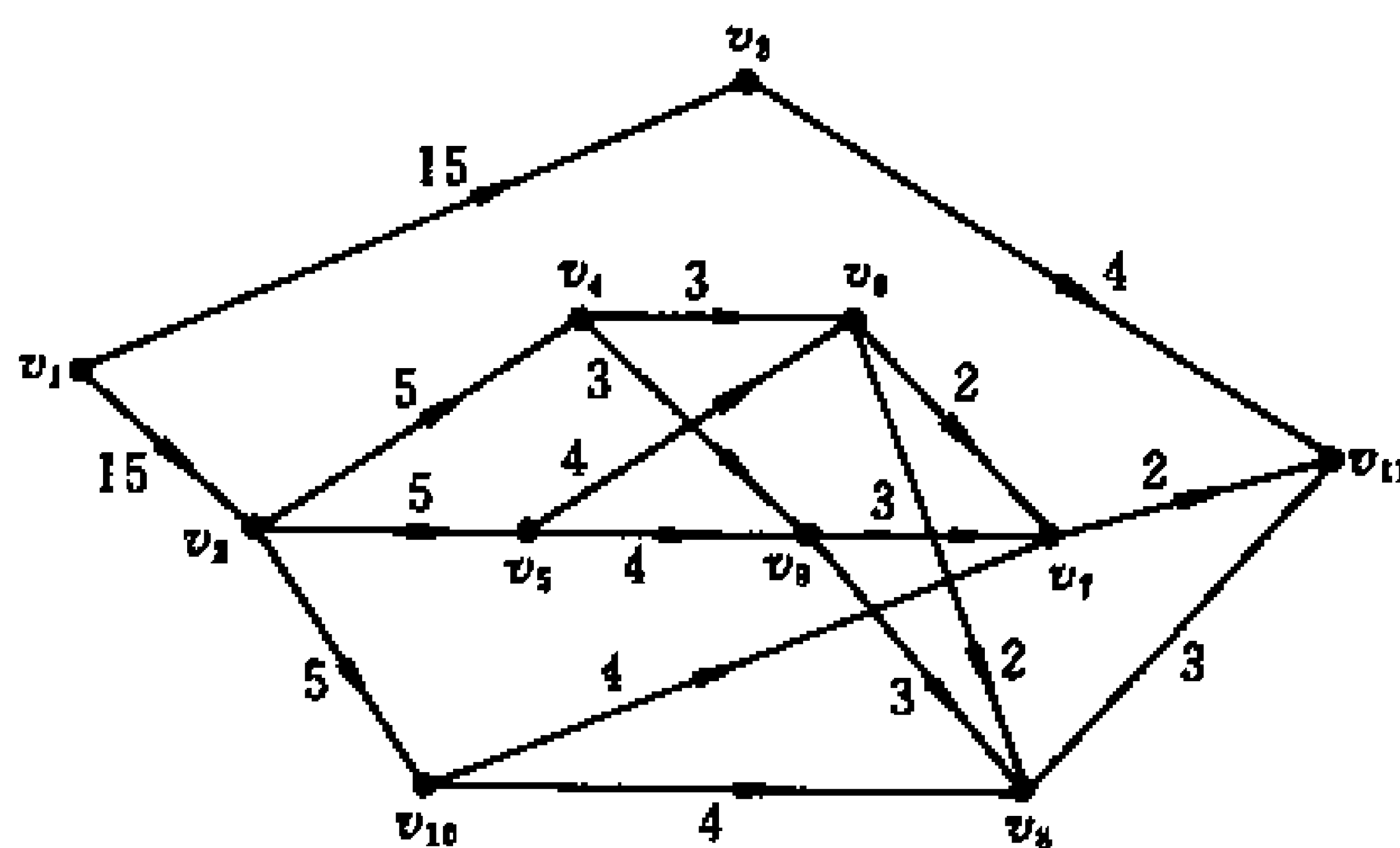


图　2.26

这种图必定不存在有向回路，否则某些工序将在自身完成之后才能开始，这显然不符合实际情况。

引理 2.7.1 不存在有向回路的图 G 中，一定存在负度及正度为零的结点。

证明：在 G 中构造一条极长的有向道路 P，设 P 的始点为 v_i，终点为 v_j，就有 $d^-(v_i)=0$，$d^+(v_j)=0$。假定 $d^-(v_i)\neq 0$，则一定有边 $(v_k,v_i)\in E(G)$，若 $v_k\in P$，那么 G 存在有向回路；若 $v_k\notin P$，则 P 不是极长道路。因此 $d^-(v_i)=0$。同理可证 $d^+(v_j)=0$。

在 PT 图中增加两个虚拟结点 v_0 和 v_n，使所有负度为 0 的结点都是 v_0 的直接后继，所有正度为 0 的结点都是 v_n 的直接前趋。这些边的权都为 0，这样得到的图 G' 仍然不存在有向回路。

定理 2.7.1 设 G 不存在有向回路，可以将 G 的结点重新编号为 $v_1',v_2',\cdots,v_n'$，使得对任意的边 $(v_i',v_j')\in E(G)$，都有 $i<j$。

证明：由引理 2.7.1，G 中存在 v_i，满足 $d^-(v_i)=0$，对之重新编号为 v_1'。在 G 中删去 v_i，得到 $G'=G-v_1'$，G' 是 G 的导出子图，因此也没有负回路，这样可以将 G' 中某个负度为 0 的结点重新编号为 v'_2，再作 $G'-v_2'$，依此类推。可将 G 的全部结点重新编号。此时，G 中所有的边都是从编号小的结点指向编号大的结点，否则与编号的原则相悖。

这样编号以后，假定 v'_1 到各点的最长路径长度依次是

$0=\pi(v'_1),\pi(v'_2),\cdots,\pi(v'_n)$，

则 $\pi(v'_j)=\max_{1\le i<j}(\pi(v'_i)+w(v'_i,v'_j))$，

这就是最长路径算法的基础。

算法 1. 最长路径算法。

a. 对结点重新编号为 $v'_1,v'_2,\cdots,v'_n$。

b. $\pi(v'_1)\leftarrow 0$。

c. 对 j 从 2 到 n，令

$$\pi(v'_j)=\max_{v'_i\in\Gamma^-v'_j}(\pi(v'_i)+w(v'_i,v'_j))。$$

d. 结束。

由于结点编号时只判别负度为 0 的结点，如果已经求出每个结点的负度，那么当需要删除 v_i（即对 v_i 重新编号）时，则 v_i 直接后继的负度都减 1。因为 $\sum_{v_i\in V}d^-(v_i)=m$，所以步骤 a 需要 m 次减法和判断。同理，在步骤 c 计算 $\pi(v'_j)$ 时，只要判断它的直接前趋 v'_i，所以 c 总共需要 m 次加法和比较。综上算法 1 的计算复杂性是 $O(m)$。

由前所述，算法 1 所得到的最长路径是一条关键路径。其长度即是整个工程最早的完工时间。因此，这条路径上的工序是不能延误的，否则将影响工程的完成。但是对于不在关键路径上的工序，是否允许延误？如果允许，最多能够耽误多长时间呢？

设 $\pi(v_n)$ 是工程完工的最早时间，工序 i 的最晚启动时间应该是

$$\tau(v_i)=\pi(v_n)-\pi(v_i,v_n)，$$

其中 $\pi(v_i,v_n)$ 表示 v_i 到 v_n 的最长路长度。

v_i 到 v_n 的最长路径等于 G 的转置 G'（即其权矩阵的转置所对应的图）中 v_n 到 v_i 的最长路径。因此把 G 的各边方向倒置而权值不变就得到 G'。由于 G 不含有向回路，故 G' 也不含有向回路。所以 G' 中 v_n 到各点的最长路径同样可以调用算法 1 实现，从而得到每个结点 v_i 的最晚启动时间 $\tau(v_i)$。

是否还有更好的计算方法呢？我们发现算法 1 步骤 a 执行之后，由于每个结点 v'_i 到结点 v'_n 的最长路径长度可以按如下公式计算：

$$\pi(v'_i,v'_n)=\max_{v'_j\in\Gamma^+(v'_i)}(\pi(v'_j,v'_n)+w(v'_i,v'_j))，$$

因而只要对结点采用逆序，依次求出 $\pi(v'_n,v'_n)=0,\pi(v'_{n-1},v'_n),\cdots$，就可以实现。于是得到

算法 2. （已知结点重新编号）

a. $\tau(v'_n)=\pi(v'_n)$。

b. 对 j 从 $(n-1)$ 到 1，令

$$\tau(v'_i)=\min_{v'_j\in\Gamma^+(v'_i)}(\tau(v'_j)-w(v'_i,v'_j))。$$

c. 结束。

这样 G 中每个结点 v_i 都具有 2 个值：最早启动时间 $\pi(v_i)$ 和最晚启动时间 $\tau(v_i)$。显然工序 i 的允许延误时间是 $t(v_i)=\tau(v_i)-\pi(v_i)$。

例 2.7.2 对例 2.7.1 的各结点的重新排序如图 2.27，其最早启动时间是

$\pi(1')=0,\ \pi(2')=15,\ \pi(3')=15,$

$\pi(4')=20,\ \pi(5')=20,\ \pi(6')=24,$

$\pi(7')=24,\ \pi(8')=20,\ \pi(9')=27,$

$\pi(10')=27,\ \pi(11')=30$。

最晚启动时间是

$\tau(11')=30,\quad \tau(10')=27,$

$\tau(9')=28,$

$\tau(8')=23, \tau(7')=24,$

$\tau(6')=25, \tau(5')=20, \tau(4')=21,$

$\tau(3')=26, \tau(2')=15, \tau(1')=0$。

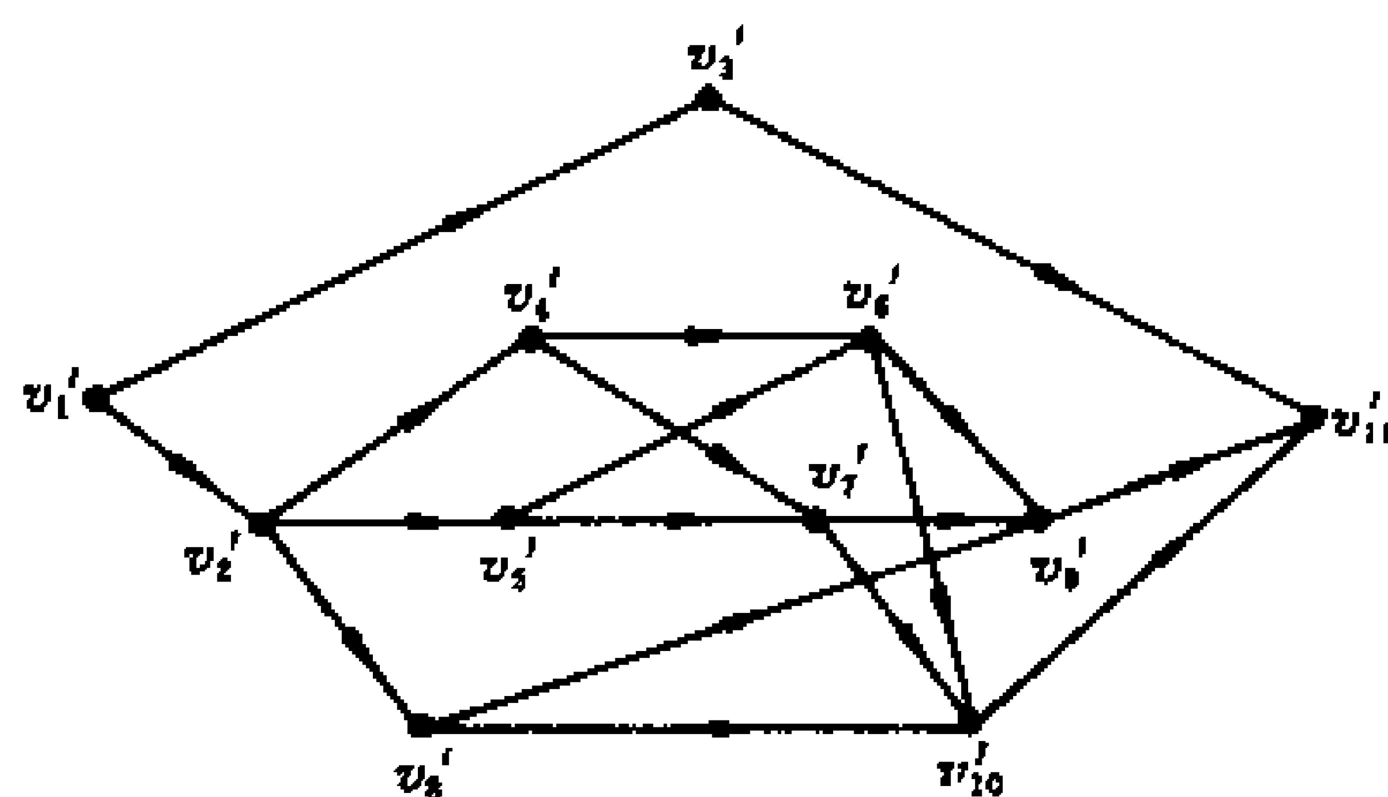


图 2.27

因而图 2.26 各工序的允许延误时间是

$t_1=0, t_2=0, t_3=11, t_4=1, t_5=0,$

$t_6=1, t_7=1, t_8=0, t_9=0, t_{10}=3, t_{11}=0$。

从中可见，最长路径即关键路径上各工序是不允许延误的，否则必将拖延整个工程的进度。

2.7.2 PERT 图

在 PERT(Programme evaluation and review technique)图中，采用有向边表示工序，其权值表示该工序所需时间。如果工序 e_i 完成后 e_j 才能开始，则令 v_k 是 e_i 的终点，e_j 的始点。根据这种约定，例 2.7.1 的 PERT 图如 2.28，其中$\underline{i}$表示工序 i。

同样，PERT 图不存在有向回路。而且与 PT 图类似，PERT 图中工程的最早完工时间是 v_1 到 v_n 的最长路径长度，这条路径就是关键路径。工序 $e_k=(v_i,v_j)$的最早启动时间是 $\pi(v_i)$，最晚启动时间是 $\tau(v_i,v_j)=\pi(v_n)-\pi(v_j,v_n)-w(v_i,v_j)$，其中 $\pi(v_j,v_n)$ 是 v_j 到 v_n 的最长路径长度，$w(v_i,v_j)$是该工序所需的时间。这样工序 $e_k=(v_i,v_j)$的允许延误时间是 $t(v_i,v_j)=\tau(v_i,v_j)-\pi(v_i)$。

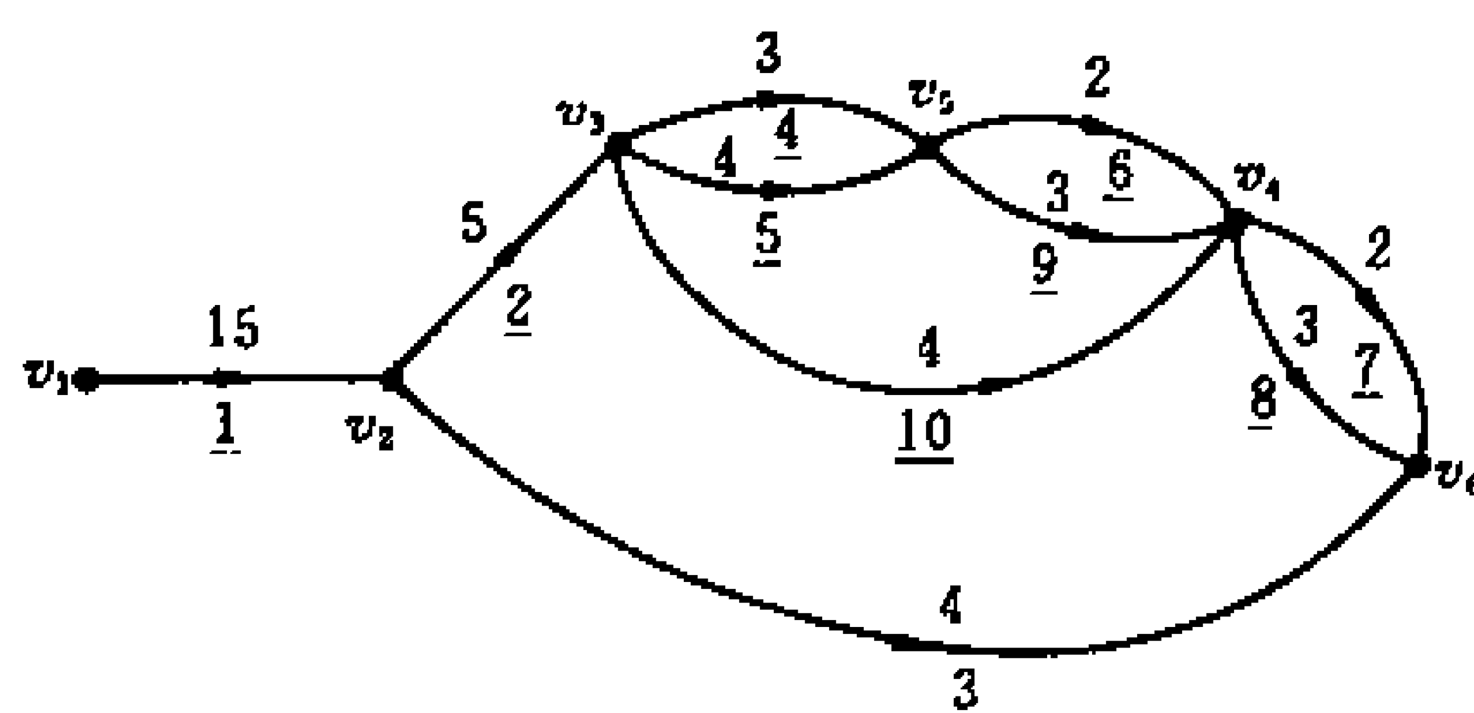


图 2.28

由算法 1 可以求出 $\pi(v_i')$，为了便于计算 $t(v_i',v_j')$，可先作简单变换。由于 $\tau(v_i')=\pi(v_n')-\pi(v_j',v_n')$，故 $\tau(v_i',v_j')=\tau(v_j')-w(v_i',v_j')$，即得 $t(v_i',v_j')=\tau(v_j')-\pi(v_i')-w(v_i',v_j')$。这样可直接使用算法 2 求 $\tau(v_j')$。以图 2.28 为例，其计算结果是(设已回到原结点号)。

$\pi(1)=0,\ \pi(2)=15,\ \pi(3)=20,\ \pi(4)=27,\ \pi(5)=24,\ \pi(6)=30,$

$\tau(1)=0,\ \tau(2)=15,\ \tau(3)=20,\ \tau(4)=27,\ \tau(5)=24,\ \tau(6)=30,$

$t(\underline{1})=0,\ t(\underline{2})=0,\ t(\underline{3})=11,\ t(\underline{4})=1,\ t(\underline{5})=0,\ t(\underline{6})=1,$

$t(\underline{7})=1, t(\underline{8})=0, t(\underline{9})=0, t(\underline{10})=3$。

与 PT 图一样，采用 PERT 图计算关键路径的复杂性也是 $O(m)$。

PT 图和 PERT 图各具特色。PERT 图包含的结点和边数少些，而 PT 图的结点数与 PERT 图的边数基本相同。因此当边数 m 较大时 PERT 图有其优越性。不过 PT 图更加灵活，它能适应一些额外的约束。例如图 2.29 中

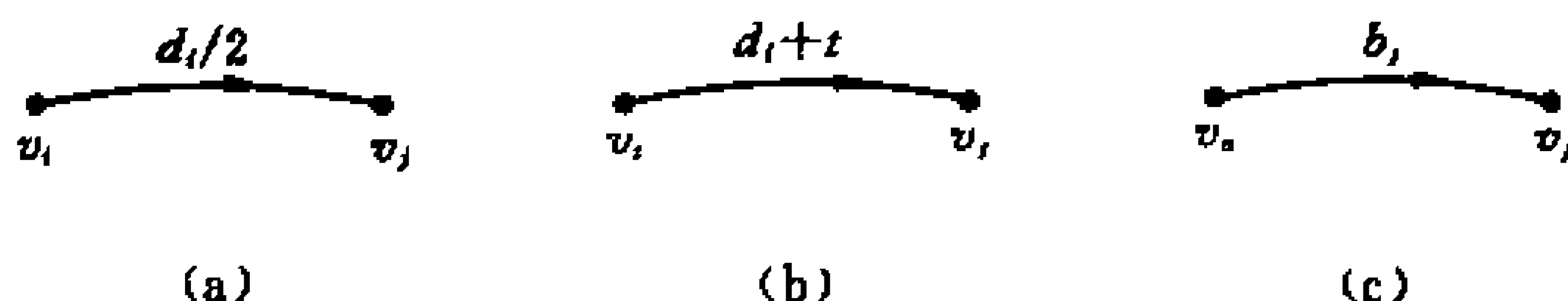


图 2.29

(a) 表示工序 i 完成一半之后 j 就可以开始。

(b) 表示工序 i 完成后经过 t 时刻 j 才开始。

(c) 表示在时间 b_j 之后工序 j 才能开始，其中 v_0 表示虚拟结点。

2.8 中 国 邮 路

中国邮路问题是我国著名图论学者管梅谷教授首先提出并解决的。它与欧拉回路、最短路以及最小费用流问题都有密切联系。

邮递员传送报纸和信件，要从邮局出发经过他所管辖的每一条街道最后返回邮局，当然每个邮递员都希望选择一条最短的传送线路，这就是中国邮路问题。用图论的语言描述，就是在一个正权连通图 G 中，求从某结点出发经过每条边至少一次最后返回出发点的最短回路。

我们分别对 G 是无向连通图和有向连通图进行讨论，而混合图的求解较为复杂，本书不再加以分析。

2.8.1 无向图的中国邮路

如果 G 中各结点的度都是偶数，那么 G 一定有欧拉回路。显然任何一条欧拉回路都是该问题的解。若 G 中只有 2 个结点 v_i, v_j 的度是奇数，则一定存在从 v_i 到 v_j 的一条欧拉道路，它经过了 G 的各边一次。在 G 中再找一条从 v_j 到 v_i 的最短道路 P_{ji}，则 $G'=G+P_{ji}$ 中存在欧拉回路。这样 G' 中的欧拉回路，即对应于 G 中 P_{ji} 的边重复一次而其余边只过一次的回路是一条中国邮路、或称最佳邮路。

如果 G 中度为奇数的结点数多于 2 个，怎样确定最佳邮路呢？

定理 2.8.1 L 是无向连通图 G 最佳邮路的充要条件是：

1. G 的每条边最多重复一次。

2. 在 G 的任意一个回路上，重复边的长度之和不超过该回路长度的一半。

证明：必要性。如果一条最佳邮路要重复经过某些边，我们将 G 中 k 次重复的边画出相应的 k 条边，得到 G'，假定一条最佳邮路 L' 使 G 中的任一条边 e_{ij} 重复 $n(n\geqslant 2)$ 次，这时

G'中有欧拉回路 L'。若使 e_{ij}在 G 中重复 $n-2$ 次，得到 G''，G'' 各点的度仍是偶数，G''的欧拉回路 L''也是 G 的一条中国邮路，且 $\pi(L'')<\pi(L')$。与 L'是最佳邮路矛盾，因此 L'中 e_{ij} 最多重复一次。假定 G 的某个回路 C 上重复边的总长超过该回路长度的一半，可以令 C 中重复边不重复，不重复边重复，得到 G'' 仍是欧拉图。但 $\pi(L'')<\pi(L')$，亦与 L'是最佳邮路矛盾。

充分性。假定任意两个不同的邮路 L_1，L_2 都满足条件 1 和 2，我们将证明 $\pi(L_1)=\pi(L_2)$。假定此式成立，因为最佳邮路 L'也满足 1 和 2，这样 $\pi(L')=\pi(L_1)$，即 L_1 和 L_2 都是最佳邮路。于是充分性就能得证。

设 $L_1=E(G)+Q+Q_1$，$L_2=E(G)+Q+Q_2$，其中 Q 是 L_1 和 L_2 中共同的重复边集合。Q_1 是只属于 L_1，Q_2 是只属于 L_2 的重复边集合。L_1 和 L_2 的对称差 $E'(G)=Q_1+Q_2$ 是 G 中只属于 L_1 和只属于 L_2 的重复边集合。构造 $G'=(V(G),E'(G))$，G'是简单图，且各结点的度都是偶数。若 $E'(G)=\Phi$，显见 $\pi(L_1)=\pi(L_2)$；否则 G' 可以划分成若干个回路，对 G'的任意一个回路 C，设 C_1，C_2 分别是 L_1 和 L_2 的重复边集，由已知条件，$\pi(C_1)\leqslant\pi(C_2)$，$\pi(C_2)\leqslant\pi(C_1)$。故 $\pi(C_1)=\pi(C_2)$。因此 $\pi(L_1)=\pi(L_2)$。

定理 2.8.1 给出了求 G 中最佳邮路的构造方法。首先找出度为奇数的结点，然后依据条件 1 构造邮路，保证计算重复边之后各结点的度都是偶数，再由条件 2 对所有回路进行判断，如果发现某个回路不满足条件，则令该回路中原先重复的边不重复，而不重复边变为重复。待完全满足条件 2 时，该图的中国邮路得解。

例 2.8.1 图 2.30(a)中国邮路的求解过程如下，其中(d)是最终解。重边表示原图该边重复。

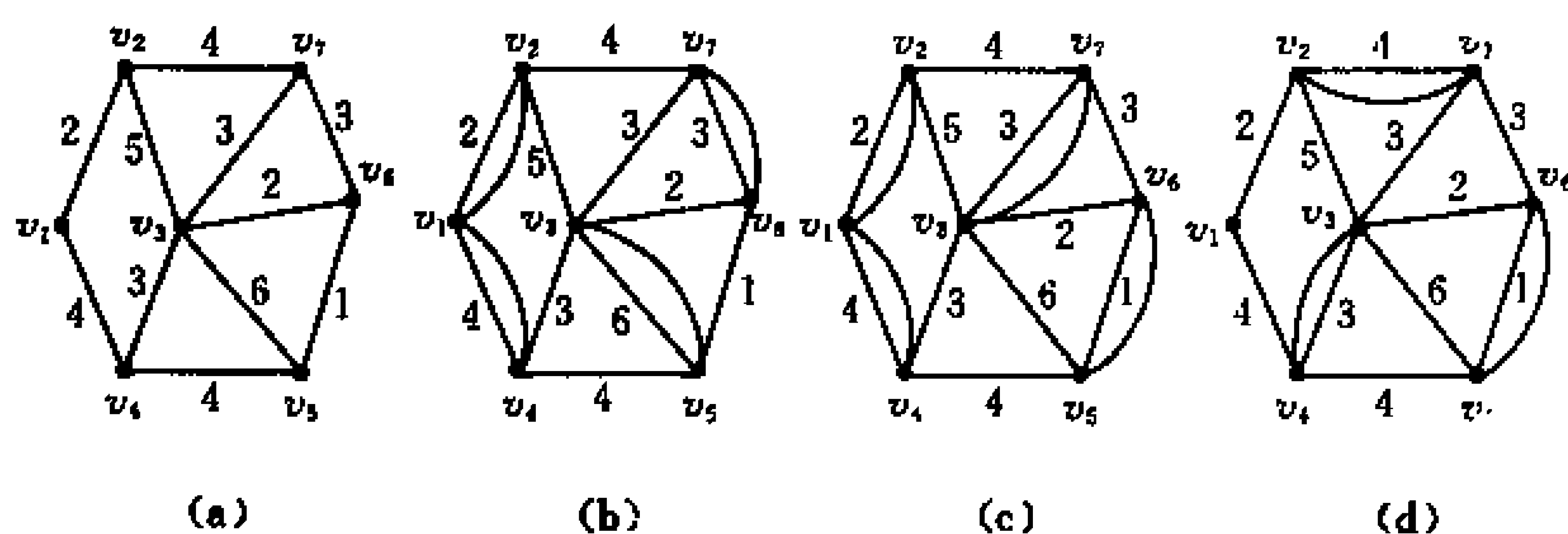


图 2.30

这种构造算法中由于回路的数量一般很多，因此计算量庞大。中国邮路问题的一个好算法是 Edmonds 提出的最小权匹配算法。最小权匹配属于运筹学范畴，在此我们只介绍该算法的基本思路。

1. 确定 G 中度为奇数的结点，构成 $V_0(G)$。

2. 求 $V_0(G)$各结点在 G 中的最短路径 P_{ij}及其长度 $\pi(v_i,v_j)$。

3. 对 $V_0(G)$的结点进行最小权匹配，即选出 $|V_0(G)|/2$ 个 $\pi(v_i,v_j)$，保证每个结点 $v_i\in V_0(G)$在 P_{ij}中只出现一次，同时满足这些 $\pi(v_i,v_j)$的总和最小。

4. 在最小权匹配里各 $\pi(v_i,v_j)$所对应的路径 P_{ij}中的诸边在 G 中重复一次，得到 G'。

5. G'是欧拉图，它的一条欧拉回路即为解。

2.8.2 有向图的中国邮路

对于有向图来说，中国邮路问题可能无解。其原因是 G 中可以含有正度或负度为 0 的结点。例如图 2.31 中就不存在最佳邮路。以下我们将排除这类情况进行讨论。

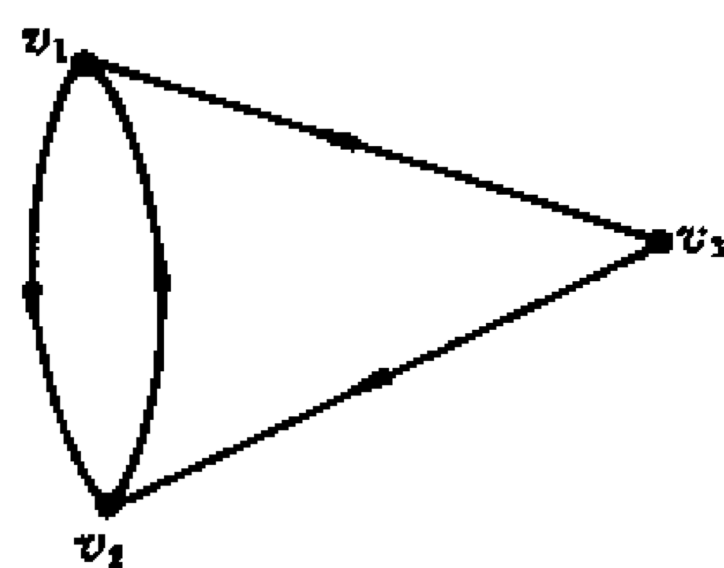


图 2.31

如果 G 中各结点的正、负度相等，则由推论 2.3.2，G 中存在有向欧拉回路。它过每边一次且仅一次。因此任一条欧拉回路都是中国邮路。

如果图 G 不对称，即存在一些结点 v_i，$d^+(v_i)\neq d^-(v_i)$。不妨设 $d^+(v_i)<d^-(v_i)$，由于邮递员要经过进入 v_i 的每一条边，因此他一定要重复走以 v_i 为始点的某条边。设 f_{ij} 表示边 (v_i,v_j) 的重复次数，w_{ij} 表示该边的权，那么中国邮路要选择重复一些边后存在有向欧拉回路并且使

$$\sum_{(i,j)\in E(G)} w_{ij} f_{ij}。 \tag{1}$$

为最小的一个解。显然这时满足

$$d^-(v_i)+\sum_j f_{ji} = d^+(v_i)+\sum_j f_{ij}, \qquad v_i\in V(G)$$

将上式整理可得

$$\sum_j (f_{ij}-f_{ji}) = d^-(v_i)-d^+(v_i) = d'(i)。 \tag{2}$$

如果 $d'(i)>0$，表示邮路中 v_i 要 $d'(i)$ 次重复经过 v_i 所发出的一些边，或者说 v_i 可供应 $d'(i)$ 个单位量。如果 $d'(i)<0$，表示邮路中 v_i 要 $d'(i)$ 次重复经过进入 v_i 的一些边，或者说 v_i 可接收 $d'(i)$ 个单位量。$d'(i)=0$ 则称 v_i 是中间结点。由于 $\sum d^+(v_i)=\sum d^-(v_i)$，所以 $\sum d'(i)=0$。这样可以逐次保证每个可供应点 v_i 经过一些边向某个接收点 v_j 供应 1 个单位量，最后达到平衡。或者说这些道路上的边出现重复，最后得到的图 G' 是有向欧拉图。如果这些重复边的总长最小，它即是最佳邮路。

为了便于分析，可以对图 G 增设两个结点：超发点 v_s，超收点 v_t。对每一个供应点 v_i，都有边 (v_s,v_i)，$f_{si}=d(i)$，$w_{si}=0$；对每一个接收点 v_j，都有边 (v_j,v_t)，$f_{jt}=-d(j)$，$w_{jt}=0$。如果用 $|d(i)|$ 条重边表示 (v_s,v_i)，$|d_j|$ 条重边表示 (v_j,v_t)，得到多重图 G'。这样中国邮路问题导致求过 G' 中形如 (v_s,v_i)，(v_j,v_t) 每边一次，总长最短的 $d(v_s)$ 条 P_{st} 道路。

综上，非对称有向图的中国邮路算法的基本思路是：

1. 计算各结点的正、负度，求出 $d'(i)$。

2. 添加一个超发点 v_s，对满足 $d'(i)>0$ 的结点 v_i，加入 $d'(i)$ 条有向边 (v_s,v_i)，权均为 0；添加一个超收点 v_t，对满足 $d'(j)<0$ 的结点 v_j，加入 $|d'(j)|$ 条有向边 (v_j,v_t)，权均为 0。得到图 G'。

3. 在 G' 中求 $d(v_s)$ 条过以 v_s，v_t 为两端点的形如 (v_s,v_i)，(v_j,v_t) 每边一次且仅一次的总和最小的 P_{st} 道路。记下 G 中各边在这些道路中的重复次数。

4. 计入各边的重复次数，G 中存在有向欧拉回路，其中一条即为解。

现举例说明如下：

例 2.8.2 求图 2.32 的中国邮路。

解:(1) 各结点的 $d'(i)$为 $d'(1)=d'(5)=0, d'(2)=2, d'(3)=-1, d'(4)=-1$。

(2) 构造 G'如图 2.33(a)。

(3) 得到 2 条总和最小的 P_{st}道路 $P_1=(v_s, v_2, v_4, v_t)$,$\pi(P_1)=5$。$P_2=(v_s, v_2, v_4, v_3, v_t)$,$\pi(P_2)=6$。$\sum\pi(p_i)=11$。这样边$(v_2,v_5)$重复 2 次,边$(v_4,v_3)$重复 1 次。得图 2.33(b),其中虚线边表示重复 1 次。

(4) 2.33(b)是欧拉图。其中一条欧拉回路如$(v_1, v_2, v_4, v_3, v_2, v_4, v_3, v_5, v_2, v_4, v_5, v_1)$就是最佳邮路。

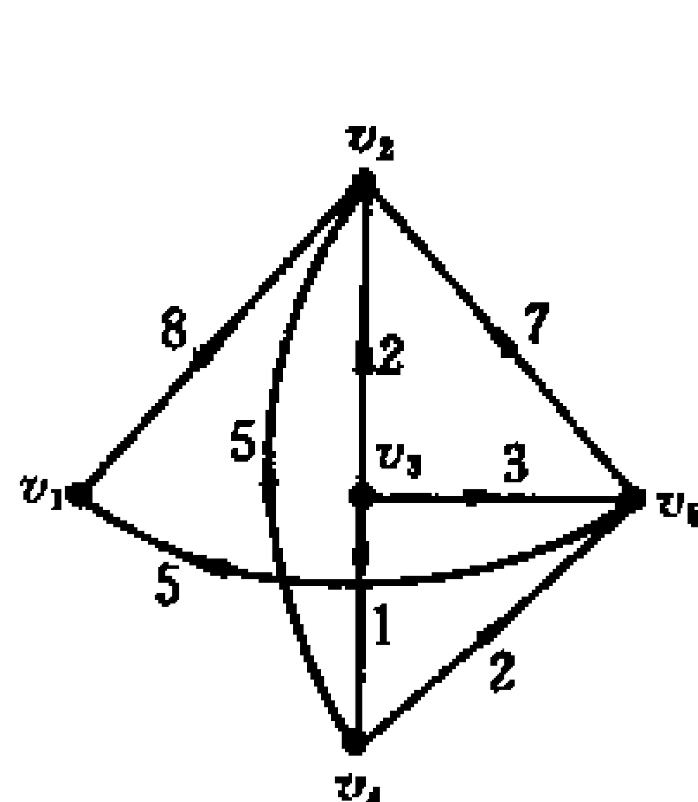
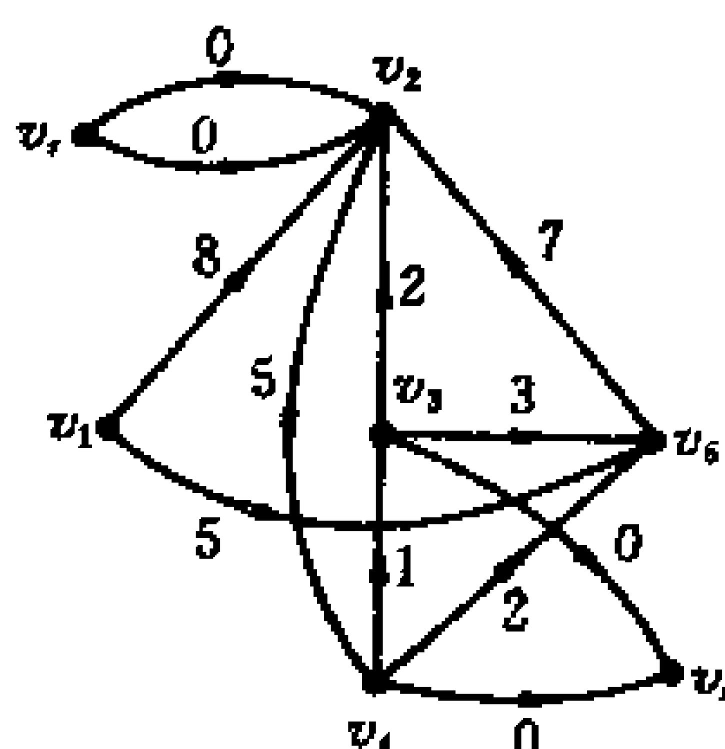


图 2.32



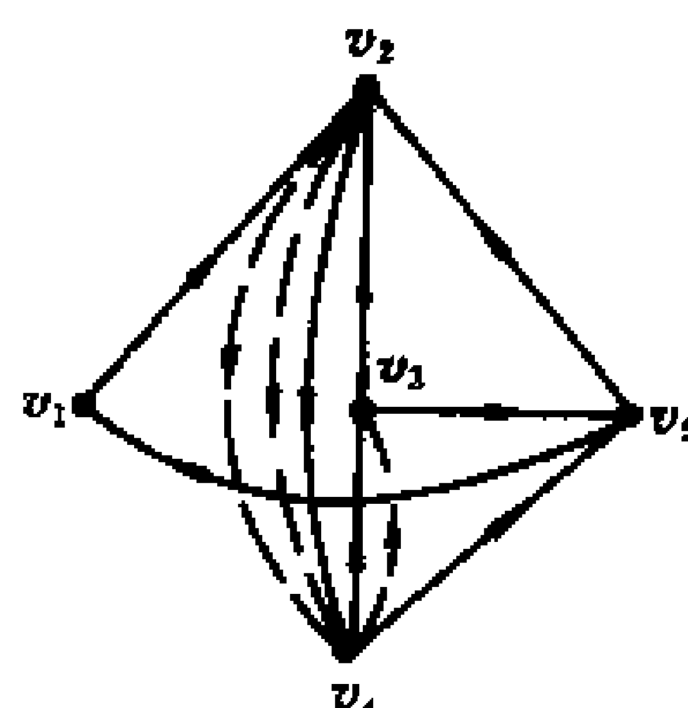


图 2.33

算法的难点是步骤 3。它需要找 $d(v_s)$条 P_{st}道路,这些道路长度的总和最小。若用 Dijkstra算法一条一条地寻找最短 P_{st}道路,则计算量比较大,同时结果并不一定最佳。如果我们把 G 中每边的权视为通过该边的费用,而容量为∞,对始发点 v_s,(v_s, v_i)形式的边只有一条,它的费用为 0,容量为 $d'(i)$;同样对超收点 v_t,每条边(v_j, v_t)的费用为 0,容量为$|d'(j)|$,这样步骤 3 就可以转化为在 G'上求从 v_s 到 v_t 传送$\sum d'(i)$个单位量的最小费用流问题,如式(1)所示。关于最小费用流将在第六章讨论。

习 题 二

1. 设简单图 G 有 k 个连通支,证明

$$m\leqslant\frac{1}{2}(n-k+1)(n-k)。$$

2. 证明 G 和 $\overline{G}$ 至少有一个是连通图。

3. 证明:连通图有的最长道路必定相交于同一结点。

4. 在简单图中,证明:若 $n\geqslant4$ 且 $m\geqslant2n-3$,则 G 中含有带弦的回路。

5. 设 G 是不存在三角形的简单图,证明:

   a. $\sum d^2(v_i)\leqslant mn$。

   b. $m\leqslant\frac{n^2}{4}$。

6. 房间的俯视图如题图 2.6，问是否存在一条路过各门一次？试说明理由。

题图 2.6

7. 设 G 有 H 道路，证明对任意 $S\subset V(G)$，$G\text{-}S$ 的连通支数 $t\leqslant|S|+1$。

8. 设 G 是 $n\geqslant3$ 的简单图，证明：若

$$m\geqslant\frac{1}{2}(n-1)(n-2)+2,$$

则 G 存在 H 回路。

9. 设 G 是有向完全图，证明 G 中存在有向的哈密顿道路。

10. 在例 2.4.5 中，若 $n\geqslant4$，证明这 n 个人一定可以围成一圈，使相邻者互相认识。

11. 设 G 是有 n 个结点的简单图，其最小度 $\delta(G)\geqslant\frac{n+q}{2}$，证明 G 中存在包含任意 q 条互不相邻边的哈密顿回路。

12. 对一个 3×3×3 的立方体，能否从一个角上开始，通过所有 27 个 1×1×1 的小立方块各 1 次，最后达到中心？试说明理由。

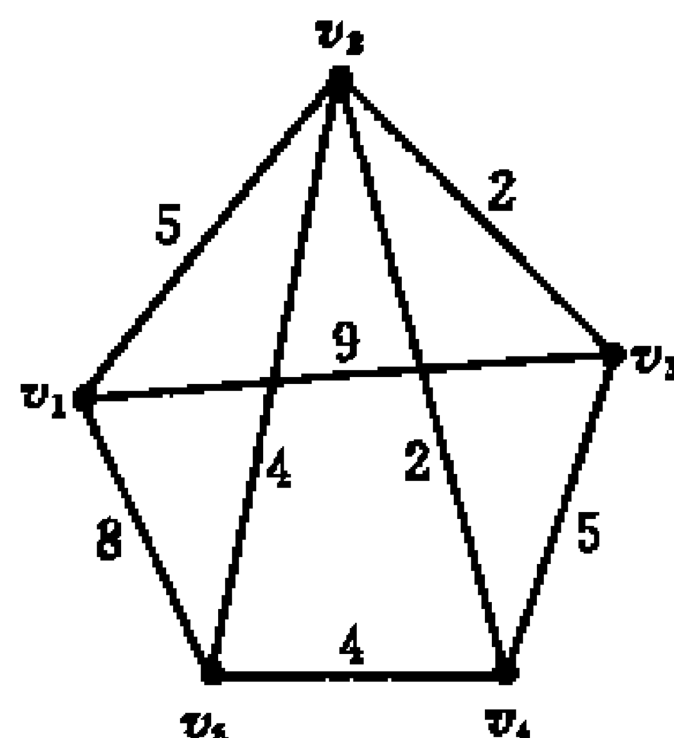
13. 已知 G 的权矩阵，用分支与界法求其旅行商问题的解

$$\begin{bmatrix} 0 & 42 & 33 & 52 & 29 \\ 42 & 0 & 26 & 38 & 49 \\ 33 & 26 & 0 & 34 & 27 \\ 52 & 38 & 34 & 0 & 35 \\ 29 & 49 & 27 & 35 & 0 \end{bmatrix}$$

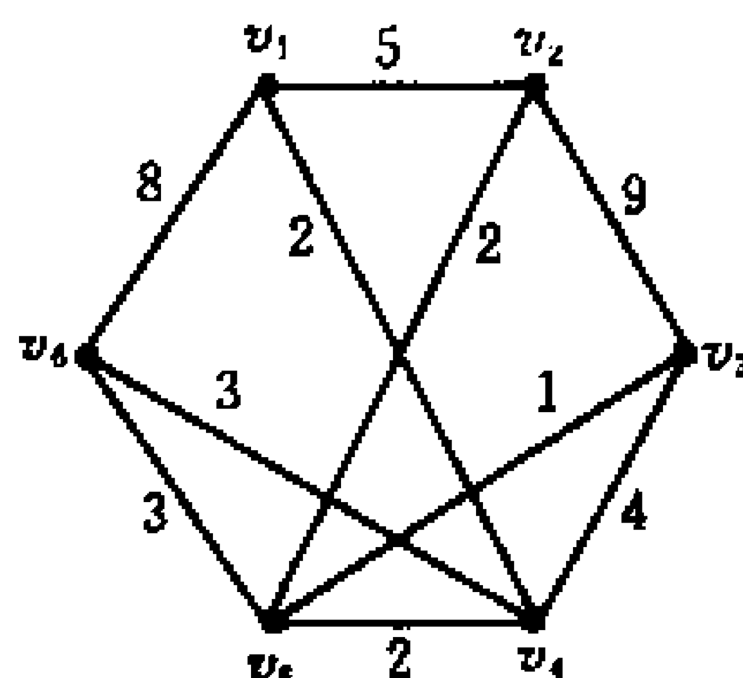
14. 一个装置从原点出发，要分别在坐标(2,5)，(9,3)，(8,9)，(6,6)停留，然后返回原点。设该装置只能沿 X 轴和 Y 轴行进，求最短的行进路线。

15. 某设备今后五年的价格预测分别是(5,5,6,7,8)，若该设备连续使用，其第 $i(i=1,2,\cdots,5)$年的维修费分别是(1,2,3,5,6)。某单位今年购进一台，问如何使用可使 5 年里总开支最小？

16. 分别求图 a、b 的中国邮路。



(a)



(b)

题图 2.16

17. 一项工程，其各工序所需时间与约束关系如下表，试用(a)：PT 图与(b)：PERT 图求其关键路径。并求工序 3，5，10 的允许延误时间如表：

工序号	时间	前序工序
1	5	
2	8	1,3
3	3	1
4	6	3
5	10	2,3
6	4	2,3
7	8	3
8	2	6,7
9	4	5,8
10	5	6,7

18. 请对 Warshall 算法进行适当修改，以便在计算道路矩阵后，可以查知任意两结点间具体的路径。

19. 编程并搜索出图 2.13 的全部不同的 H 回路。

20. 试编写无负长回路图的最短路径程序。

21. 编写求 PERT 图关键路径及工序允许延误时间的程序。

22. 编写用分支与界法求旅行商问题的程序。

23. 用近似算法求权矩阵如下的旅行商问题，并与程序运行结果比较。

$$\begin{bmatrix} \times & 42 & 33 & 52 & 29 & 45 \\ 42 & \times & 26 & 38 & 49 & 36 \\ 33 & 26 & \times & 34 & 27 & 43 \\ 52 & 38 & 34 & \times & 35 & 30 \\ 29 & 49 & 27 & 35 & \times & 41 \\ 45 & 36 & 43 & 30 & 41 & \times \end{bmatrix}$$

第三章　树

3.1　树的有关定义

给定一个图 $G=(V,E)$，如果它不含任何回路，我们就叫它是林。如果 G 又是连通的，即这个林只有一个连通支，就称它是树。树是图论中最重要的概念之一，在自然科学和社会科学的许多领域都有广泛的应用。

例 3.1.1　网球单打比赛前，当抽签之后为说明各选手间的相遇情况，往往画一张图，形如图 3.1。它是一棵树。

例 3.1.2　中子袭击原子核时产生的裂变过程，也可以形象地用图 3.2 示意，它也是一棵树。

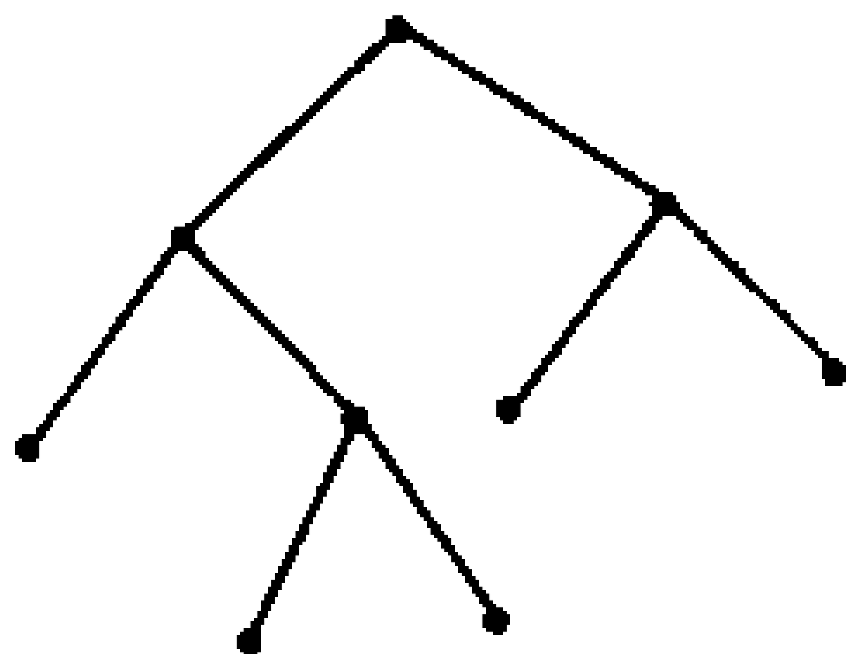


图　3.1

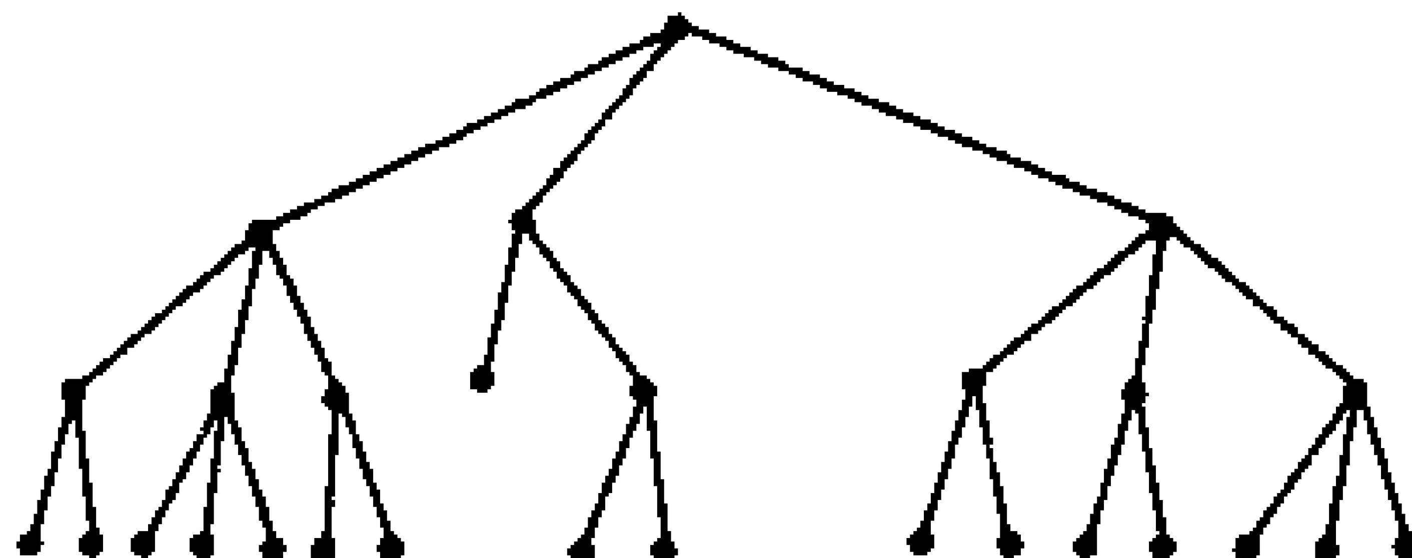


图　3.2

定义 3.1.1　一个不含任何回路的连通图称为树，用 T 表示。T 中的边称为树枝，度为 1 的结点称为树叶。

树的每条边都不会属于任何回路。这样的边叫割边。

定义 3.1.2　设 e 是 G 的一条边，若 $G'=G-e$ 比 G 的连通支数增加，则称 e 是 G 的一条割边。

显然，图 G 删去割边 $e=(u,v)$ 之后，结点 u 和 v 分属于不同的连通支。

定理 3.1.1　$e=(u,v)$ 是割边，当且仅当 e 不属于 G 的任何回路。

证明：若 $e=(u,v)$ 属于 G 的某个回路，则 $G'=G-e$ 中仍存在 u 到 v 的道路，故结点 u 和 v 属于同一连通支，e 不是割边。反之，若 e 不是割边，则 G' 与 G 的连通支数一样。于是 u 和 v 仍属于同一连通支。故 G' 中存在道路 $P(u,v)$，$P(u,v)+e$ 就是 G 的一个回路。

下面我们给出树的等价定义。

定理 3.1.2　设 T 是结点数为 $n\geqslant 2$ 的树，则下列性质等价：

1. T 连通且无回路。
2. T 连通且每条边都是割边。
3. T 连通且有 $n-1$ 条边。
4. T 有 $n-1$ 条边且无回路。
5. T 的任意两结点间有唯一道路。

6. T 无回路，但在任两结点间加上一条边后恰有一个回路。

证明：

1→2　T 无回路，即 T 的任意边 e 都不属于回路，由定理 3.1.1，e 是割边。

2→3　对结点数 n 进行归纳。令 $n(T)$，$m(T)$ 分别表示树 T 的结点数与边数。当 $n=2$ 时命题成立，设 $n\leqslant k$ 时，$m(T)=n(T)-1$ 成立。则 $n=k+1$ 时，由于任一边 e 都是割边，故 $G'=G-e$ 有两个连通支 T_1，T_2。由于 $n(T_i)\leqslant k$，$i=1,2$，故 $m(T_i)=n(T_i)-1$。所以 $m(T)=n(T)-1$ 也成立。

3→4　假定 T 有回路，设 C 是其中一条含有 $k(<n)$ 个结点的初级回路。因为 T 连通，所以 $V(T)-V(C)$ 中一定有结点 u 与 C 上某点 v 相邻，即存在边 $(u,v)\in E(T)$，依此类推，最终 $V(T)-V(C)$ 中的 $n-k$ 个结点需要 $n-k$ 条边才可能保持 T 连通，但 $|E(T)-E(C)|=n-1-k<n-k$。矛盾。

4→5　设 u，v 是 T 的任意两结点，先证道路 $P(u,v)$ 的存在性。如果不存在 $P(u,v)$，则 u，v 属于不同连通支 T_1、T_2。由 $m(T)=n-1$，则至少有一个支，比如 T_1，使 $n(T_1)\leqslant m(T_1)$ 成立。这样 T_1，亦即 T 中有回路。反之，若 T 无回路，则因为各连通支都有 $m(T_i)\leqslant n(T_i)-1$，从而使 $m(T)<n-1$。均产生矛盾，因此 $P(u,v)$ 一定存在。再证唯一性。若存在两条不同的道路 $P(u,v)$，$P'(u,v)$，则其对称差 $P(u,v)\oplus P'(u,v)$ 至少含有一个回路。故而得证。

5→6，6→1　均显然。因此等价定理得证。

定理 3.1.2 对判断和构造树 T 将带来很大方便。

定理 3.1.3　树 T 中一定存在树叶结点。

证明：由于 T 是连通图，所以任一结点 $v_i\in V(T)$，都有 $d(v_i)\geqslant 1$。若无树叶，则 $d(v_i)\geqslant 2$。这样 $n-1=m=\frac{1}{2}\sum d(v_i)\geqslant n$。矛盾。

定义 3.1.3　如果 T 是图 G 的支撑子图，而且又是一棵树，则称 T 是 G 的一棵支撑树，或称生成树，又简称为 G 的树。

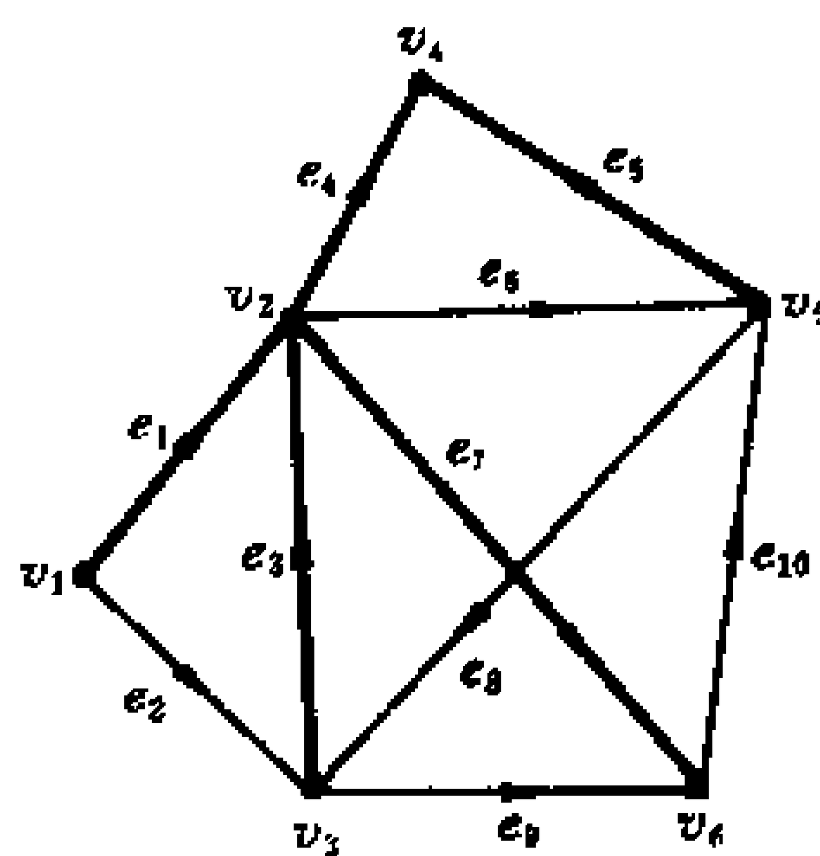


图 3.3

比如图 3.3 的粗线边构成了 G 的一棵支撑树 T。显然 G 有支撑树的充要条件为 G 是连通图，而且如果连通图 G 本身不是树，那么它的树不唯一，例如图 3.3 中还有许多不同的支撑树。给定图 G 的一棵树 T，我们称 $G-T$，即 G 删去 T 中各边后的子图为 T 的余树，用 $\overline{T}$ 表示。比如在图 3.3，$E(\overline{T})=\{e_2,e_6,e_8,e_9,e_{10}\}$。一般情况下，余树不是一棵树。

3.2　基本关联矩阵及其性质

本节讨论的对象是有向连通图 G。

定义 3.2.1　在有向图连通 $G=(V, E)$ 的关联矩阵 B 中划去任意结点 v_k 所对应

的行，得到一个 $(n-1)\times m$ 的矩阵 B_k，B_k 称为 G 的一个基本关联矩阵。

例如图 3. 3 中结点 v_6 所对应的基本关联矩阵是

$$B_6 = \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix}\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ -1 & 0 & -1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 1 & 0 & -1 \end{bmatrix}$$
$$\quad e_1 \quad e_2 \quad e_3 \quad e_4 \quad e_5 \quad e_6 \quad e_7 \quad e_8 \quad e_9 \quad e_{10}$$

基本关联矩阵与 G 的支撑树之间有密切联系。我们首先分析关联矩阵的性质。

定理 3. 2. 1 有向图 $G=(V,E)$ 关联矩阵 B 的秩 ran $B<n$。

证明：由于 B 中每列都只有 1 和 -1 两个非零元素，故 B 的任意 $n-1$ 行加到第 n 行上后，第 n 行为全零。即 B 的 n 个行向量线性相关，故 ran $B<n$。

定理 3. 2. 2 设 B_0 是有向图 G 关联矩阵 B 的任意一 k 阶子方阵，则 det (B_0) 为 0，1 或 -1。

证明：因为 B_0 是 B 的某一 k 阶子阵，显然 B_0 每列最多只有 2 个非零元。若其中某列全为零元，则 det $(B_0)=0$；若 B_0 每列都有 2 个非零元，显然也有 det $(B_0)=0$；否则 B_0 中存在只有 1 个非零元的列，按该列展开得到 det (B_1) = {±det (B_0)，但 B_1 的阶为 $k-1$。依次类推，可知最终 det (B_0) 或为 0，或为 1，或为 -1。

定理 3. 2. 3 设 B 是有向连通图 G 的关联矩阵，则 ran $B=n-1$。

证明：由定理 3. 2. 1 知 ran $B<n$，现只需证 ran $B\geqslant n-1$。不失一般性，设 B 中最少的线性相关的行数为 l，显然 $l\leqslant n$，而且这 l 行分别与结点 $v(i_1)$，$v(i_2)$，…，$v(i_l)$ 相对应，因此有

$$k_1b(i_1)+k_2b(i_2)+\cdots+k_lb(i_l)=0 \qquad k_j\neq 0, j=1,2,\cdots,l \tag{1}$$

由于矩阵 B 每列只有 2 个非零元，所以在这 l 个行向量 $b(i_j)$ 中，其第 $t(t=1,2,\cdots,m)$ 个分量最多只有 2 个为非零。当然也可能全为 0。但是可以断言：不可能只有 1 个为非零。否则，由于 $k_j\neq 0$，式(1)不会成立。这样可以对矩阵 B 分别进行行、列交换，使前 l 行是线性相关的诸行；这在 l 行中每列都有 2 个非零元的换到前 r 列，其余 $m-r$ 列它们全都是零元。这样矩阵 B 变换为

$$B'=\begin{bmatrix} P & 0 \\ 0 & Q \end{bmatrix}\begin{matrix} l \\ n-l \end{matrix}$$
$$\quad r \qquad m-r$$

但 ran B' = ran B，而且 B' 依然是 G 的一个关联矩阵，与 B 相比只是结点与边的编号不同而已。若 $n-l>0$，由 B' 可见，G 至少分为 2 个连通支：其中 r 条边只与 l 个结点相关，而其余 $m-r$ 条边只与另外 $n-l$ 个结点相关。这与 G 是连通图矛盾，因此一定有 $n-l=0$，即 $l=n$，也就是说 B 中最少需要 n 行才能线性相关，而任何 $n-1$ 行都将线性无关，因此 ran $B\geqslant n-1$。

由此，我们立刻得到

定理 3.2.4 连通图 G 基本关联矩阵 B_k 的秩 ran $B_k=n-1$。

推论 3.2.1 n 个结点树 T 的基本关联矩阵的秩是 $n-1$。

树是包含边数最少的连通图。对于连通图 G，显然满足 $m \geqslant n-1$。既然连通图基本关联矩阵 B_k 的秩是 $n-1$，那么 B_k 中一定存在 $n-1$ 个线性无关的列，究竟哪些列会是线性无关的，哪些列又必定线性相关呢？

定理 3.2.5 设 B_k 是连通图 G 的基本关联矩阵，C 是 G 中的一个回路。则 C 中各边所对应 B_k 的各列线性相关。

证明：只需针对 C 是初级回路进行讨论，设 C 包含了 G 的 l 个结点 l 条边，(不妨 $l<n$)，这 l 条边对应关联矩阵 B 的 l 列，它们构成 B 的子阵 $B(Gc)$。由于 C 本身也是连通图，所以 $B(C)$ 是 l 阶方阵，而 ran $B(C)=l-1$，故 $B(C)$ 的 l 列线性相关，但它又是 $B(Gc)$ 的子阵。由于 $B(Gc)$ 对应的各边只经过回路 C 的结点，因此 $B(Gc)$ 中其余结点所对应的行元素全为零。这样，$B(Gc)$ 的 l 列仍是线性相关，显然 $B_k(Gc)$ 的各列也线性相关。

推论 3.2.2 设 H 是连通图 G 的子图，如果 H 含有回路，则 H 的诸边对应的 G 的基本关联矩阵各列线性相关。

定理 3.2.6 令 B_k 是有向连通图 G 的基本关联矩阵，那么 B_k 的任意 $n-1$ 阶子阵行列式非零的充要条件是其各列所对应的边构成 G 的一棵支撑树。

证明：必要性。如果某个 $n-1$ 阶子阵 $B_k(G_T)$ 的行列式非零。则由推论 3.2.2，T 中不含回路，它包含 n 个结点，$n-1$ 条边，根据定理 3.1.2 的等价定义 4，T 是 G 的一棵树。充分性。设 T 是 G 的一棵树，子图 T 的基本关联矩阵 $B_k(T)$ 是 $n-1$ 阶的方阵，其行列式非零，它又恰好对应 B_k 的某个 $n-1$ 阶子阵，即 B_k 所对应的该 $n-1$ 阶行列式非零。

定理 3.2.6 说明图 G 基本关联矩阵中行列式非零的 $n-1$ 阶子阵的数目与 G 不同的支撑树数目之间存在一种对应关系。

3.3 支撑树的计数

本节讨论连通图 G 中支撑树的数目以及根树的数目。

定理 3.3.1 (Binet-Cauchy 定理)已知两个矩阵 $A=(a_{ij})_{m\times n}$ 和 $B=(b_{ij})_{n\times m}$，满足 $m\leqslant n$，则 $\det(AB)=\sum_i A_iB_i$，其中 A_i，B_i 都是 m 阶行列式，A_i 是从 A 中取不同的 m 列所成的行列式，B_i 是从 B 中取相应的 m 行构成的行列式，然后再对全部组合求和。

定理的证明从略。现举一例进行说明和验证。

例 3.3.1 已知

$$A=\begin{bmatrix} 4 & 3 & 2 \\ -2 & 4 & 3 \end{bmatrix} \qquad B=\begin{bmatrix} 5 & 1 \\ 0 & 3 \\ 4 & 2 \end{bmatrix}$$

求 $\det(AB)$。

解：由矩阵乘法

$$AB=\begin{bmatrix} 28 & 17 \\ 2 & 16 \end{bmatrix}$$

所以 $\det(AB)=414$。由比内——柯西定理计算，

$$\det(AB) = \sum_i A_i B_i$$
$$= \begin{vmatrix} 4 & 3 \\ -2 & 4 \end{vmatrix}\begin{vmatrix} 5 & 1 \\ 0 & 3 \end{vmatrix} + \begin{vmatrix} 4 & 2 \\ -2 & 3 \end{vmatrix}\begin{vmatrix} 5 & 1 \\ 4 & 2 \end{vmatrix} + \begin{vmatrix} 3 & 2 \\ 4 & 3 \end{vmatrix}\begin{vmatrix} 0 & 3 \\ 4 & 2 \end{vmatrix}$$
$$= 414。$$

从例中显然可见，用比内——柯西定理计算乘积矩阵的行列式比通常的方法复杂，但该定理揭示了乘积矩阵的行列式与各矩阵的子阵行列式之间的关系，连通图 G 不同支撑树的计数恰好利用了这种关系，从而使计数问题很容易地得到解决。下面针对不同的对象分别讨论树的计数。

3.3.1 有向连通图的树计数

定理 3.3.2 设 B_k 是有向连通图 $G=(V,E)$ 的某一基本关联矩阵，则 G 的不同树的数目是 $\det(B_kB_k^T)$。

证明：设 $B_k=(b_{ij})_{(n-1)\times m}$，由于 G 是连通图，故 $n-1\leqslant m$，由比内——柯西定理

$$\det(B_kB_k^T) = \sum_i |B_i||B_i^T|。 \tag{1}$$

其中 $|B_i|$ 是 B_k 的某一 $n-1$ 阶子阵的行列式，$|B_i^T|$ 是对应的 B_k^T 的 $n-1$ 阶子阵的行列式，由于 B_k^T 是 B_k 的转置矩阵，所以 $|B_i^T|$ 的第 j 行正好是 $|B_i|$ 的第 j 列，亦即 $|B_i|=|B_i^T|$，(1)式可写成

$$\det(B_kB_k^T) = \sum_i |B_i|^2。 \tag{2}$$

由定理 3.2.6，如果 $|B_i|\neq 0$，则其所对应的边构成 G 的一棵树，由定理 3.2.2，此时 $|B_i|=1$ 或 -1，因此 $|B_i|^2=1$。这说明如果 B_i 的各列所对应的边构成 G 的一棵树，则对 $\det(B_kB_k^T)$ 中的贡献为 1。而式(2)是对 $|B_i|^2$ 的全部组合求和。因此 $\det(B_kB_k^T)$ 恰是 G 中不同树的数目。

例 3.3.2 求图 3.4 的树的数目。

解：任取一个基本关联矩阵，比如 B_4，

$$B_4=\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ -1 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

$$\therefore \quad \det(B_4B_4^T)=\det\begin{bmatrix} 2 & -1 & 0 \\ -1 & 3 & -1 \\ 0 & -1 & 2 \end{bmatrix}=8。$$

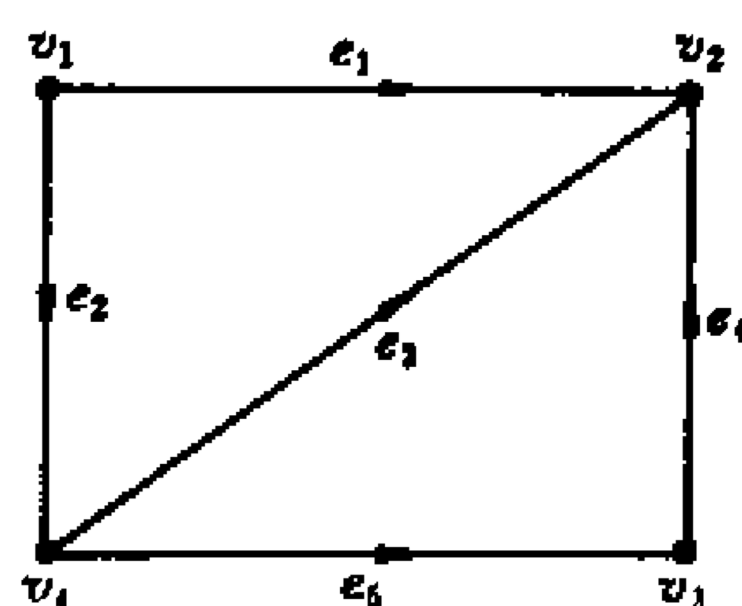


图 3.4

有时根据需要，还要计算 G 中不含或必含某特定边 $e=(u,v)$ 的树的数目。如果不含边 e，则 $G'=G-e$ 的树就与之一一对应，因此只需计算 G' 的支撑树数目。如果必含 $e=(u,v)$，可以将结点 u 和 v 收缩成一个结点，记为 uv，得到 $n-1$ 个结点的新图 G'，原图 G 中某点 t 如果与 u(或 v)相邻，则在 G' 中与结点 uv 仍相邻，且方向不变。如果 t 与 u、v 都相邻，则 G' 里 t 与 uv 之间存在 2 条有向边。这样，G' 的树就与 G 中必含 e 的树一一对应。

例 3.3.3 求图 3.4 中不含 e_4 的树数目。

解：作 $G-e_4$，得到图 3.5。

$$\det(B_4B_4^T)=\det\begin{bmatrix}2 & -1 & 0\\ -1 & 2 & 0\\ 0 & 0 & 1\end{bmatrix}=3。$$

故 G 中不含 e_4 的树有 3 棵。

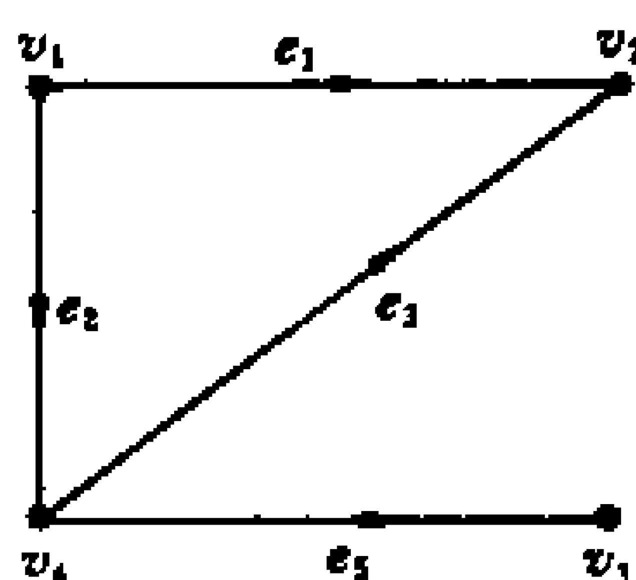


图 3.5

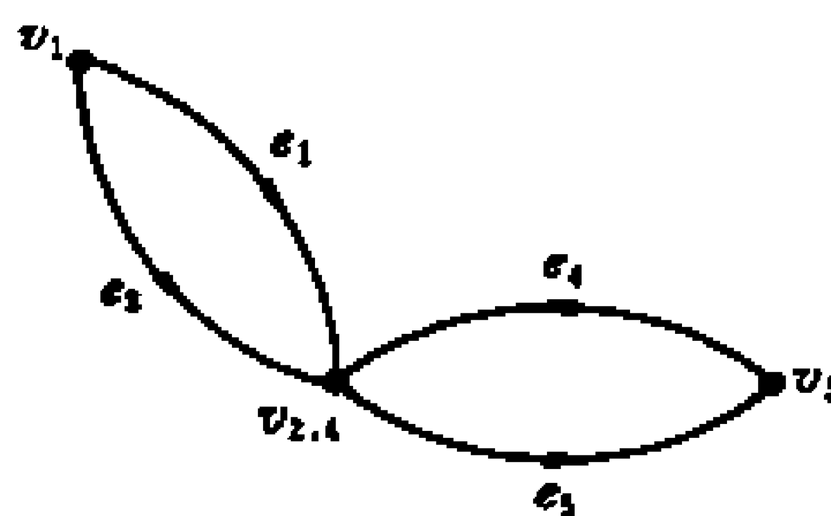


图 3.6

例 3.3.4 求图 3.4 中必含 e_3 的树数目。

解：将结点 v_2,v_4 收缩为 $v_{2,4}$，得到图 3.6。

$$\det(B_3B_3^T)=\det\begin{bmatrix}2 & -2\\ -2 & 4\end{bmatrix}=4。$$

故 G 中必含 e_3 的树有 4 棵。

这 4 棵树显然是分别由 $\{e_1,e_4\}$，$\{e_1,e_5\}$，$\{e_2,e_4\}$，$\{e_2,e_5\}$ 构成。返回到图 G，再分别加入 e_3 就是 G 的树。

通过上述计算不难发现，$C=B_kB_k^T$ 的元素 c_{ij} 十分易求，若 $i=j$，则 $c_{ij}=d(v_i)$，即 B_k 里 v_i 所对应行中的非零元数目；若 $i\neq j$，则 $-c_{ij}$ 是图 G 中 (v_i,v_j) 或 (v_j,v_i) 形式的边数目。这对计算那些较难写出关联矩阵的图的树计数问题会带来方便。

3.3.2 无向连通图的树计数

无向连通图同样有其支撑树，但是它的关联矩阵 B 中不存在 -1 元素，因此不能直接采用比内——柯西定理的方法进行树计算。对无向连通图 G 的每边任给一方向，便得到相应的有向连通图 G'，显然 G' 的树一定与 G 的树一一对应，这样无向连通图 G 的树计数问题便迎刃而解。

例 3.3.5 求完全图 k_n 中不同树的数目。

解：对 k_n 各边任给一方向，得到有向完全图 G，设 G 中结点 v_k 所对应的基本关联矩阵是 B_k。于是可以得到

$$\det(B_kB_k^T)=\det\begin{bmatrix}n-1 & -1 & \cdots & -1\\ -1 & n-1 & & -1\\ -1 & -1 & & n-1\end{bmatrix}=n^{n-2}。$$

3.3.3 有向连通图 G 根树的计数

定义 3.3.1 T 是有向树，若 T 中存在某结点 v_0 的负度为 0，其余结点的负度为 1，

则称 T 是以 v_0 为根的外向树，或称根树，用 $\vec{T}$表示。

例如图 3.7 就是一棵根树。树根 v_0 所对应的基本关联矩阵是

$$B_0 = \begin{bmatrix} -1 & 0 & 1 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & -1 & 0 & 0 \end{bmatrix}$$

由于 v_0 的负度为 0，其余结点的负度为 1，因此任何以 v_0 为根的根树的基本关联矩阵 B_0 中一定是每行每列都只有一个 -1 元素。如果对根树的结点和边序号重新编号，使得每条边 $e=(v_i,v_j)$ 都满足 v_i 的编号小于 v_j 的编号，同时边 $e=(v_i,v_j)$ 的编号为 e_j。例如图 3.7 的重新编号可以是图 3.8。

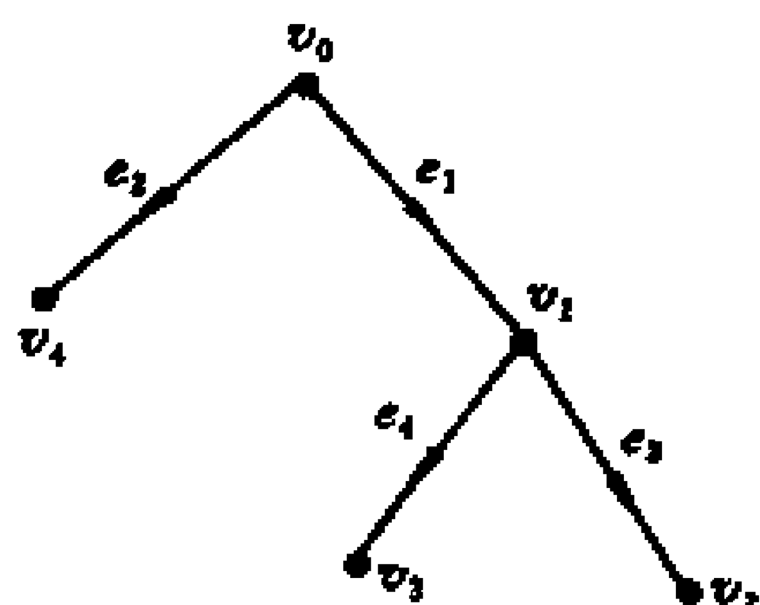


图 3.7

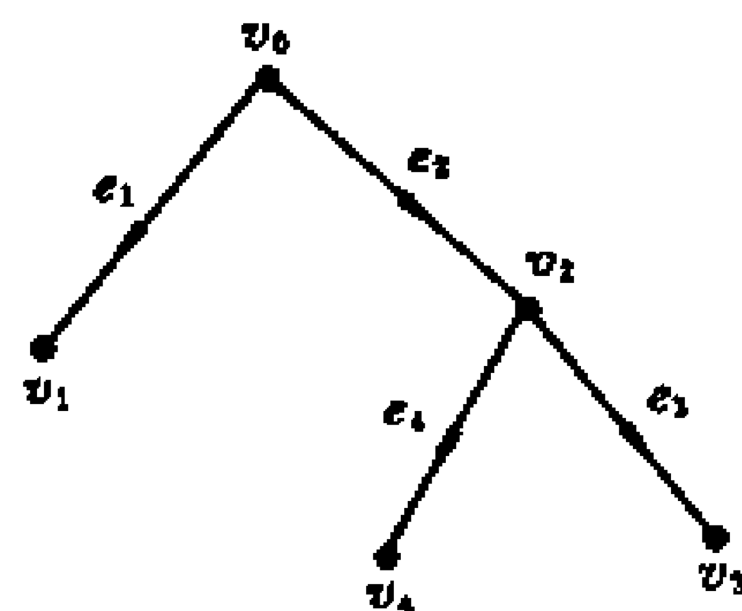


图 3.8

它的基本关联矩阵是

$$B_0' = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

事实上它只是对 B_0 的行、列分别进行若干次初等变换的结果。它们的行列式是相等的。但从 B'_0 看出，它是一个上三角方阵，-1 元全是对角元。如果把矩阵中的 1 元改为 0，它的行列式也不变。这正是根树的特征。如果 T 不是根树，它的基本关联矩阵决不会有 B'_0 的形式，因此如果把其中 1 元素改为 0，它的行列式将是 0。

令 $\bar{B}_k$ 表示有向连通图 G 的基本关联矩阵 B_k 中将全部 1 元素改为 0 之后的矩阵。我们有

定理 3.3.3 有向连通图 G 中以 v_k 为根的根树数目是 $\det(\bar{B}_k B_k^T)$

证明：由比内——柯西定理

$$\det(\bar{B}_k B_k^T) = \sum_i |\bar{B}_i| |B_i^T|,$$

若 $|B_i^T| \neq 0$，说明这 $n-1$ 条边构成 G 的一棵树，此时如果 $|\bar{B}_i| \neq 0$，说明这棵树是以 v_k 为根的根树。这时 $|\bar{B}_i| = |B_i^T|$，因此它们在 $\det(\bar{B}_k B_k^T)$ 中的贡献为 1，由于遍历了所有 $n-1$条边的组合，所以 v_k 为根的根树数目是 $\det(\bar{B}_k B_k^T)$。

例 3.3.6 计算图 3.9 中以 v_1 为根的根树数目。

解：v_1 所对应的基本关联矩阵是

$$B_1=\begin{bmatrix}-1 & 0 & 0 & 1 & 0 & 1\\ 0 & 0 & -1 & 0 & -1 & -1\\ 0 & -1 & 0 & -1 & 1 & 0\end{bmatrix}$$

$$\bar{B}_1B_1^T=\begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & -1 & 0 & -1 & -1\\ 0 & -1 & 0 & -1 & 0 & 0\end{bmatrix}\begin{bmatrix}-1 & 0 & 0\\ 0 & 0 & -1\\ 0 & -1 & 0\\ 1 & 0 & -1\\ 0 & -1 & 1\\ 1 & -1 & 0\end{bmatrix}$$

$$=\begin{bmatrix}1 & 0 & 0\\ -1 & 3 & -1\\ -1 & 0 & 2\end{bmatrix}$$

$$\therefore \qquad \det(\bar{B}_1B_1^T)=6。$$

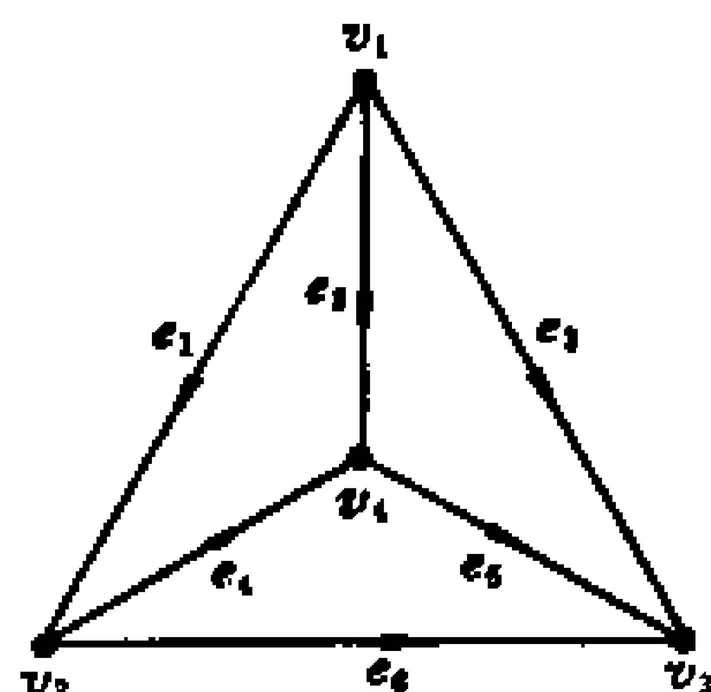


图 3.9

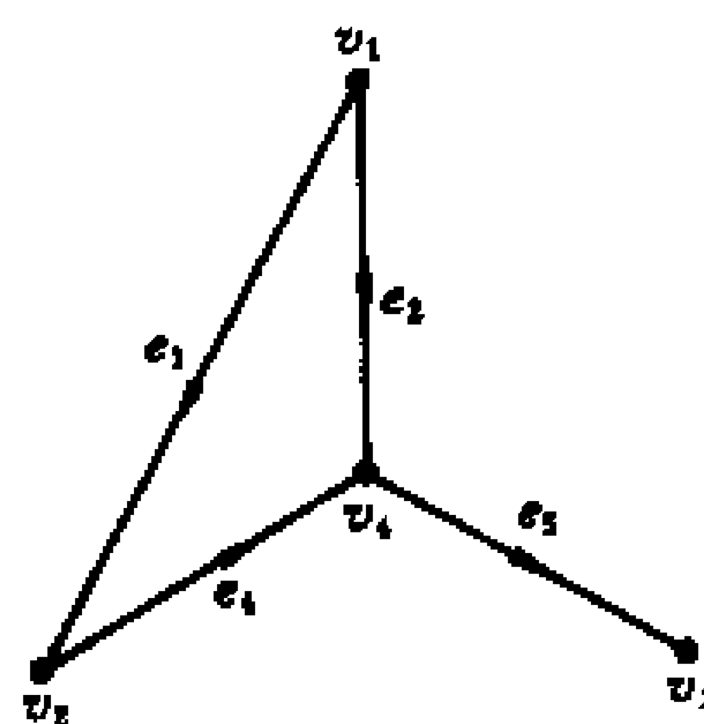


图 3.10

例 3.3.7 求图 3.9 以 v_1 为根不含边 e_5 的根树数目。

解:作 $G'=G-e$,则 G' 的以 v_1 为根的根树数目正是所求,于是

$$B_1=\begin{bmatrix}-1 & 0 & 0 & 1 & 1\\ 0 & 0 & -1 & 0 & -1\\ 0 & -1 & 0 & -1 & 0\end{bmatrix}$$

$$\det(\bar{B}_1B_1^T)=\det\begin{bmatrix}1 & 0 & 0\\ -1 & 2 & 0\\ -1 & 0 & 2\end{bmatrix}=4。$$

计算 G 中以 v_0 为根必含某特定边 $e=(u,v)$ 的根树数目,可以先计算以 v_0 为根的根树数,再计算不含 e 的根树数,其差即是。这里再介绍另一种计算方法。由于根树的特征是任意一个非根的结点 v_i,其负度都是 1。如果要求根树必含 $e=(u,v)$,即 $\vec{T}$ 中结点 v 的进入边已定,因而任何其它 (t,v) 形式的边都不会在根树中出现。所以可作 $G'=G-\{(t,v)\mid t\neq u\}$,$G'$ 中以 v_0 为根的根树数目即为所求。

例 3.3.8 求图 3.9 以 v_1 为根必含 e_5 的根树数目。

解:做 $G'=G-e_3-e_6$,得图 3.10。

$$B_1 = \begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & -1 & -1 & 1 \end{bmatrix}$$

$$\det(\bar{B}_1 B_1^T) = \det \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ -1 & 0 & 2 \end{bmatrix} = 2,$$

即 G 中有 2 棵以 v_1 为根必含 e_5 的根树。

3.4 回路矩阵与割集矩阵

有向连通图 $G=(V,E)$的回路矩阵与割集矩阵都与 G 的支撑树有密切关系，同时在网络，特别是电路网络中有广泛的应用。

3.4.1 回路矩阵及其性质

设 T 是有向连通图 $G=(V,E)$的一棵支撑树，对任意的边 $e\in E(G)-E(T)$，$T+e$ 都构成了 G 的一个唯一回路 C，如果给回路 C 确定一个参考方向，那么该回路的边，如果其方向与回路方向一致，就称它是正向边，否则称为反向边。

定义 3.4.1 有向连通图 G 的全部初级回路构成的矩阵，称为 G 的完全回路矩阵，记为 C_e，它的元素是

$$c_{ij} = \begin{cases} 1, & e_j \in C_i \text{ 且与回路 } C_i \text{ 方向一致。} \\ -1, & e_j \in C_i \text{ 且与回路 } C_i \text{ 方向相反。} \\ 0, & \text{其它。} \end{cases}$$

例 3.4.1 图 3.11 的完全回路矩阵是

$$C_e = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & -1 & 0 \\ -1 & 0 & 1 & -1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

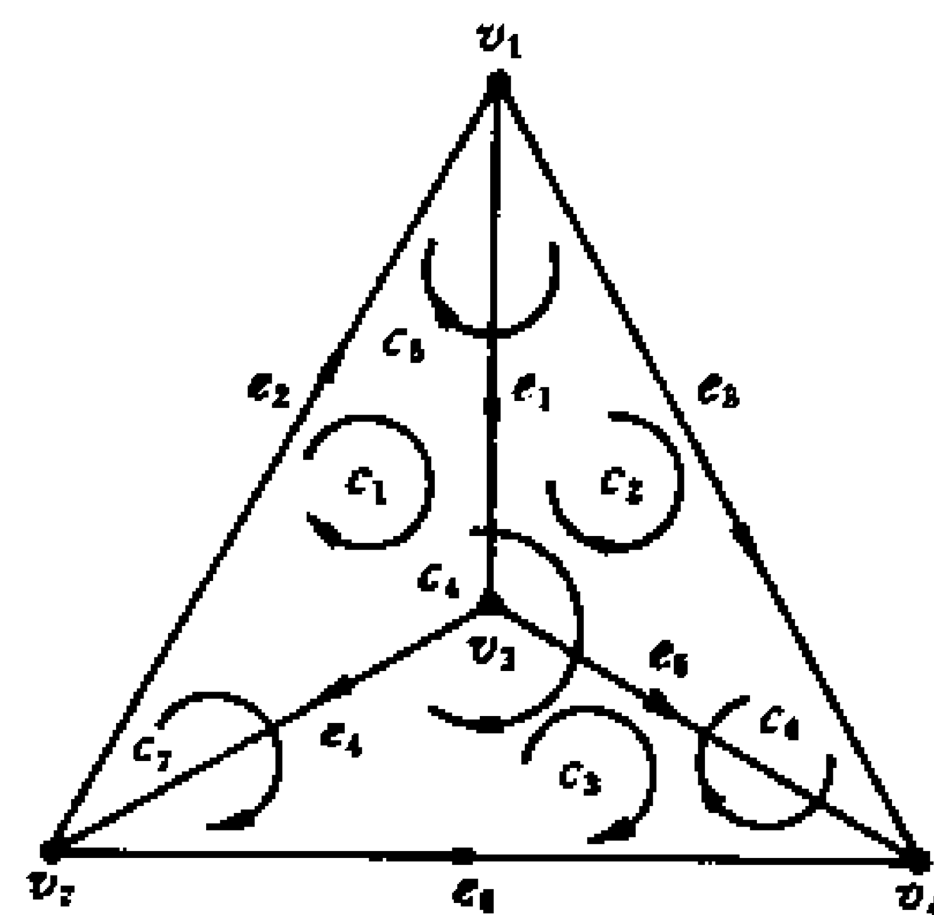


图 3.11

由于 $k(1\leqslant k\leqslant m-n+1)$条余树枝可能与 T 构成一个初级回路，因此完全回路矩阵 C_e 中最多可能包含 $2^{m-n+1}-1$ 个不同的初级回路。但是这些回路不一定都是独立的。比如上例中 $C_1\oplus C_3=C_7$。那么哪些回路是独立的呢？

定义 3.4.2 当有向图 $G=(V,E)$的树 T 确定以后，每条余树边 e 所对应的回路称为基本回路，该回路的方向与 e 的方向一致。由全部基本回路构成的矩阵称为 G 的基本回路矩阵，记为 C_f。

例 3.4.2 给定图 3.11 的一棵树 $T=\{e_1,e_5,e_6\}$，则其基本回路矩阵是

$$C_f = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ -1 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 & -1 \end{bmatrix}$$
$$\quad e_1 \quad e_2 \quad e_3 \quad e_4 \quad e_5 \quad e_6$$

显然基本回路矩阵中每个回路都是独立的，因此 $\text{ran}\ C_f = m-n+1$。进而，如果将 C_f 的行、列分别进行一下交换，使树枝边放在后，余树边放在前且次序与它所构成的回路一致，就可以写成分块矩阵形式，比如上例

$$C_f = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & -1 & -1 & 0 \\ 0 & 0 & 1 & 0 & -1 & -1 \end{bmatrix}$$
$$\quad e_2 \quad e_3 \quad e_4 \quad e_1 \quad e_5 \quad e_6$$

亦即

$$C_f = (I \quad C_{f_{12}}),$$

其中 $C_{f_{12}}$ 是树枝边所对应的子阵。

定理 3.4.1 有向连通图 $G=(V,E)$ 的关联矩阵 B 和完全回路矩阵 C_e 的边次序一致时，恒有

$$BC_e^T = 0。$$

证明：设 $D = BC_e^T, d_{ij} = \sum_{k=1}^{m} b_{ik} \cdot c_{jk}$；其中 b_{ik} 是结点 v_i 与边 e_k 的关联状况，c_{jk} 是回路 C_j 与边 e_k 的相关情况。回路 C_j 与结点 v_i 的相处只有 2 种可能：

(1) C_j 不经过 v_i，如图 3.12(a)，则与 v_i 关联的任一边都不是 C_j 中的边，所以 $d_{ij}=0$。

(2) C_j 经过 v_i，如图 3.12(b)，则必定经过与 v_i 关联的 2 条边 e_p 和 e_q，若 e_p 和 e_q 在 C_j 中方向一致，则对 v_i 来说它们是一进一出，因此 $d_{ij}=0$；如果 e_p 和 e_q 在 C_j 中方向相反，对 v_i 它们却是同进同出，同样 $d_{ij}=0$。

由于 d_{ij} 的任意性，故定理得证。

定理 3.4.2 有向连通图 $G=(V,E)$ 完全回路矩阵 C_e 的秩是 $m-n+1$。

证明：由于 C_f 是 C_e 的子阵且 $\text{ran}\ C_f = m-n+1$，故 $\text{ran}\ C_e \geqslant m-n+1$。现证 $\text{ran}\ C_e \leqslant m-n+1$，Sylvester 定理指出，两个矩阵 $A_{n\times s}$，$B_{s\times m}$，如果 $AB=0$，则 $\text{ran}\ A + \text{ran}\ B \leqslant s$。因此由定理3.4.1，得到 $\text{ran}\ B + \text{ran}\ C_e \leqslant m$，即 $\text{ran}\ C_e \leqslant m-n+1$。

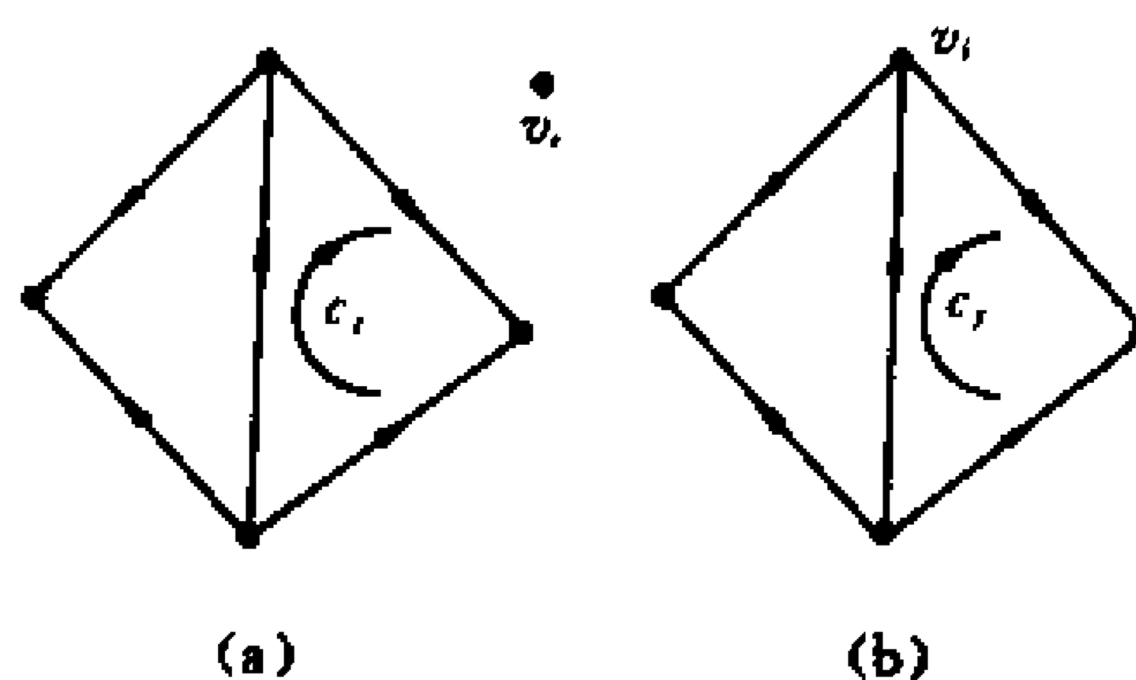


图 3.12

定义 3.4.3 由连通图 G 中 $m-n+1$ 个互相独立的回路组成的矩阵，称为 G 的回路矩阵。记为 C。

回路矩阵 C 有以下几个简单性质：

1. 基本回路矩阵 C_f 是回路矩阵。

2. $BC^T=0$，(其中 B 与 C 的边次序一致。)

3. $C=PC_f$，其中 P 是非奇异的方阵，C 与 C_f 的边次序一致。

定理 3.4.3 连通图 G 的回路矩阵 C 的任一 $m-n+1$ 阶子阵行列式非零，当且仅当这些列对应于 G 的某一棵余树。

证明：充分性。设已知 G 的某一棵余树 $\overline{T}$，则可构造基本回路矩阵 $C_f=(I \quad C_{f_{12}})$，对给定的回路矩阵 C 进行列交换，使其与 C_f 的边次序一致，这样可写成块矩阵形式 $C=(C_{11} \quad C_{12})$，其中 C_{11} 对应 $\overline{T}$。由性质 3，$C=PC_f$，即 $(C_{11} \quad C_{12})=P(I \quad C_{f_{12}})=(P \quad PC_{f_{12}})$，因此 $C_{11}=P$ 是非奇异的，即其行列式非零。再证必要性。将 C 的这 $m-n+1$ 列换到前面，成 $C=(C_{11} \quad C_{12})$。现只需证 C_{12} 对应 G 的一棵树。假设 C_{12} 对应的不是树，则一定含有回路，这种回路只由 C_{12} 中的某些边构成。这样经过行变换可得

$$C'=\begin{bmatrix} C'_{11} & C'_{12} \\ 0 & C''_{12} \end{bmatrix}$$

其中 $C''_{12}\neq 0$。于是

$$\det(C_{11})=\det\begin{bmatrix} C'_{11} \\ 0 \end{bmatrix}=0。$$

与 $\det C_{11}\neq 0$ 矛盾。

该定理揭示了 G 的余树与其回路矩阵之间的关系。

定理 3.4.4 若有向连通图 $G=(V,E)$ 的基本关联矩阵 B_k 和基本回路矩阵 C_f 的边次序一致，并设 $C_f=(I \quad C_{f12})$，$B_k=(B_{11} \quad B_{12})$，则

$$C_{f_{12}}=-B_{11}^T B_{12}^{-T}。$$

证明：由定理 3.4.1 即得 $B_k C_f^T=0$，写成块矩阵形式，有

$$(B_{11} \quad B_{12})\begin{bmatrix} I \\ C_{f_{12}}^T \end{bmatrix}=0，$$

$$B_{12}C_{f_{12}}^T=-B_{11}。$$

由于 B_{12} 对应的边构成 G 的一棵树。根据定理 3.2.6，B_{12} 存在逆矩阵 B_{12}^{-1}。由此定理得证。

本定理说明如果 B_k 已知，而且确定了一棵树。则可以直接经过计算求得 G 的基本回路矩阵 C_f。

例 3.4.3 已知图 3.11 基本关联矩阵

$$B_4=\begin{bmatrix} 1 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & -1 \\ -1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$
$$\begin{matrix} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{matrix}$$

其中 e_1,e_5,e_6 所对应的子阵行列式非零，求 C_f。

解：由 e_1,e_5,e_6 可构成 G 的一棵树。对 B_4 进行列交换，得到

$$B_4=\begin{bmatrix} -1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 & 1 & 0 \end{bmatrix}=(B_{11} \quad B_{12})。$$
$$\begin{matrix} e_2 & e_3 & e_4 & e_1 & e_5 & e_6 \end{matrix}$$

其中

$$B_{11}=\begin{bmatrix}-1 & 1 & 0\\ 1 & 0 & -1\\ 0 & 0 & 1\end{bmatrix}\quad B_{12}=\begin{bmatrix}1 & 0 & 0\\ 0 & 0 & -1\\ -1 & 1 & 0\end{bmatrix}\quad B_{12}^{-1}=\begin{bmatrix}1 & 0 & 0\\ 1 & 0 & -1\\ 0 & 1 & 0\end{bmatrix}$$

因此

$$C_{f_{12}}=-B_{11}^{T}B_{12}^{-T}=\begin{bmatrix}1 & 1 & 1\\ -1 & -1 & 0\\ 0 & -1 & -1\end{bmatrix}$$

即

$$C_f=\begin{bmatrix}1 & 0 & 0 & 1 & 1 & 1\\ 0 & 1 & 0 & -1 & -1 & 0\\ 0 & 0 & 1 & 0 & -1 & -1\end{bmatrix}$$

$$\quad e_2 \quad e_3 \quad e_4 \quad e_1 \quad e_5 \quad e_6$$

3.4.2 割集矩阵及其性质

定义 3.4.4 设 S 是有向图 $G=(V,E)$ 的边子集，若

1. $G'=(V,E-S)$ 比 G 的连通支数多 1。

2. 对任意 $S'\subset S$，G 与 $G''=(V,E-S')$ 的连通支数相同。

则称 S 是 G 的一个割集。

一般给割集 S 确定一个方向，称它是有向割集。这样 S 中的每条边 e，或者与 S 同向，或者方向相反。

例 3.4.4 图 3.13 中，$S_1=\{e_2,e_3,e_4\}$，$S_2=\{e_4,e_5\}$ 是割集，而 $S_3=\{e_6,e_7\}$ 不是割集。在 S_1 中，e_2 与 S 方向相同，而 e_3，e_4 相反。

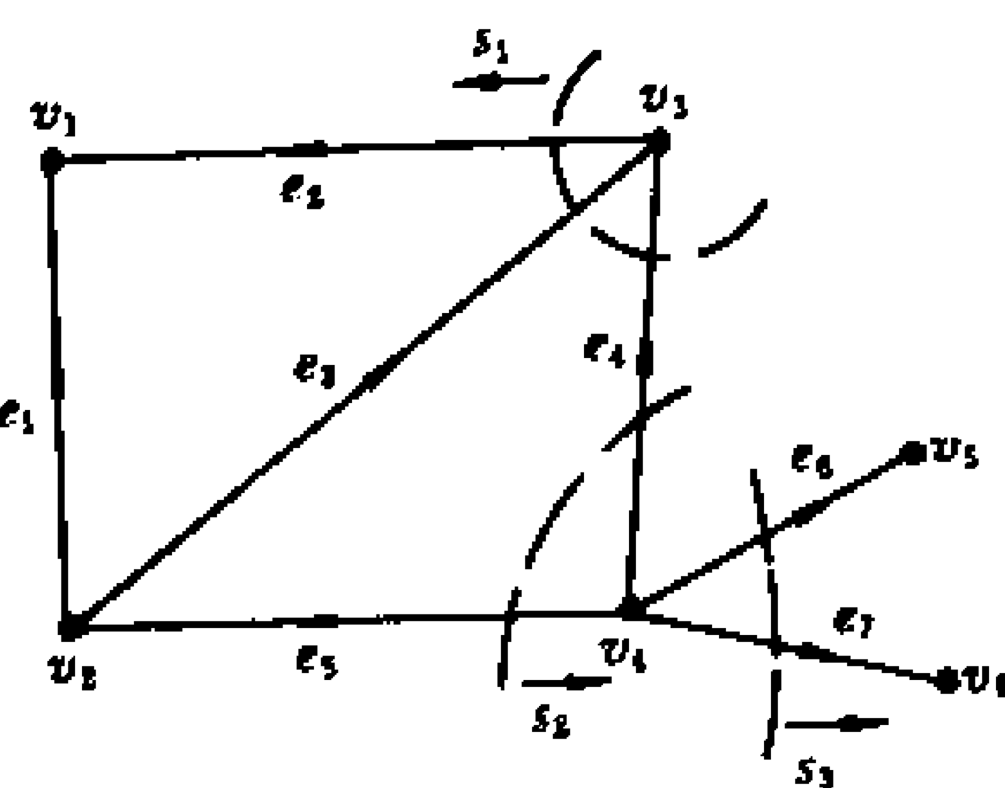


图 3.13

定义 3.4.5 有向连通图 G 的全部割集组成的矩阵，称为完全割集矩阵，记作 S_e。其元素

$$S_{ij}=\begin{cases}1, & e_j \text{ 在 } S_i \text{ 中且方向一致。}\\ -1, & e_j \text{ 在 } S_i \text{ 中且方向相反。}\\ 0, & \text{其它。}\end{cases}$$

例 3.4.5 图 3.14 的完全割集矩阵是

$$S_e=\begin{bmatrix}1 & -1 & 1 & 0 & 0 & 0\\ -1 & 0 & 0 & -1 & 0 & 1\\ 0 & 1 & 0 & 1 & 1 & 0\\ 0 & 0 & -1 & 0 & -1 & -1\\ -1 & 1 & 0 & 0 & 1 & 1\\ 1 & 0 & 1 & 1 & 1 & 0\\ 0 & -1 & 1 & -1 & 0 & 1\end{bmatrix}$$

$$\quad e_1 \quad e_2 \quad e_3 \quad e_4 \quad e_5 \quad e_6$$

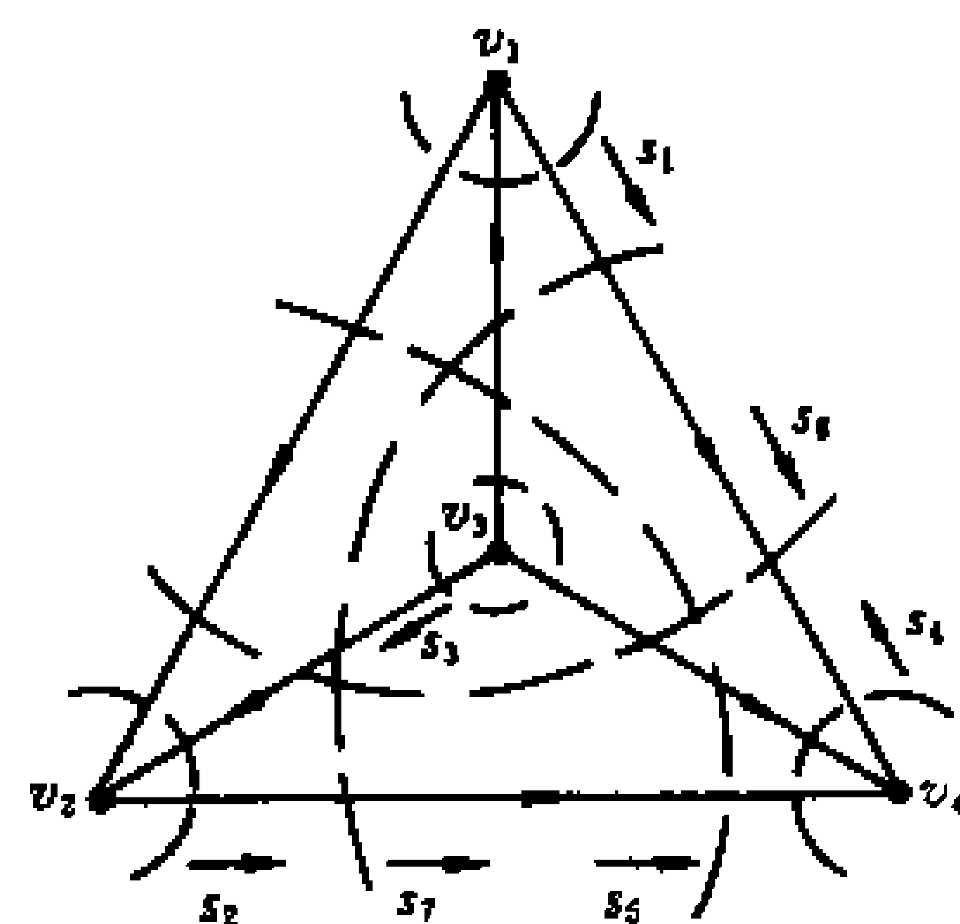


图 3.14

由于割集将连通图的结点划分成连通的两部分，其

结点数分别为 $i, n-i, 1 \leqslant i \leqslant n-1$。因此 G 最多有 $\frac{1}{2}(2^n-2)=2^{n-1}-1$ 个不同的割集。但这些割集不一定都是独立的，比如上例中 $S_7=S_1 \oplus S_2$。

定义 3.4.6 设 T 是连通图 G 的一棵树，e_i 是一个树枝。对应 e_i 存在 G 的割集 S_i，S_i 只包括一条树枝边 e_i 及某些余树枝，且与 e_i 的方向一致。这时称 S_i 为 G 的对应树 T 的一个基本割集。

定义 3.4.7 给定有向连通图 G 的一棵树 T，则由全部基本割集组成的矩阵称为基本割集矩阵。记为 S_f。

例 3.4.6 $T=\{e_2,e_3,e_4\}$ 是图 3.14 的一棵树，其基本割集矩阵是

$$S_f=\begin{bmatrix} -1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}$$
$$\quad e_1 \quad e_2 \quad e_3 \quad e_4 \quad e_5 \quad e_6$$

在基本割集矩阵中如果把余树边对应的列放在前，树枝边对应的列放在后且与割集次序一致，比如上例中

$$S_f=\begin{bmatrix} -1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 \end{bmatrix}$$
$$\quad e_1 \quad e_5 \quad e_6 \quad e_2 \quad e_3 \quad e_4$$

则基本割集矩阵可写成分块矩阵形式 $S_f=(S_{f_{11}} \quad I)$，其中单位矩阵对应一棵树。显然 $\operatorname{ran} S_f=n-1$。

定理 3.4.5 当有向连通图 G 的完全回路矩阵 C_e 和完全割集矩阵 S_e 的边次序一致时，有 $S_eC_e^T=0$。

证明：设 $D=S_eC_e^T$，$d_{ij}=\sum_{k=1}^{m} s_{ik} \cdot c_{jk}$。其中 s_{ik} 是第 i 个割集的第 k 条边、c_{jk} 是第 j 个回路的第 k 条边。割集 S_i 与回路 C_j 的相处只有 2 种。

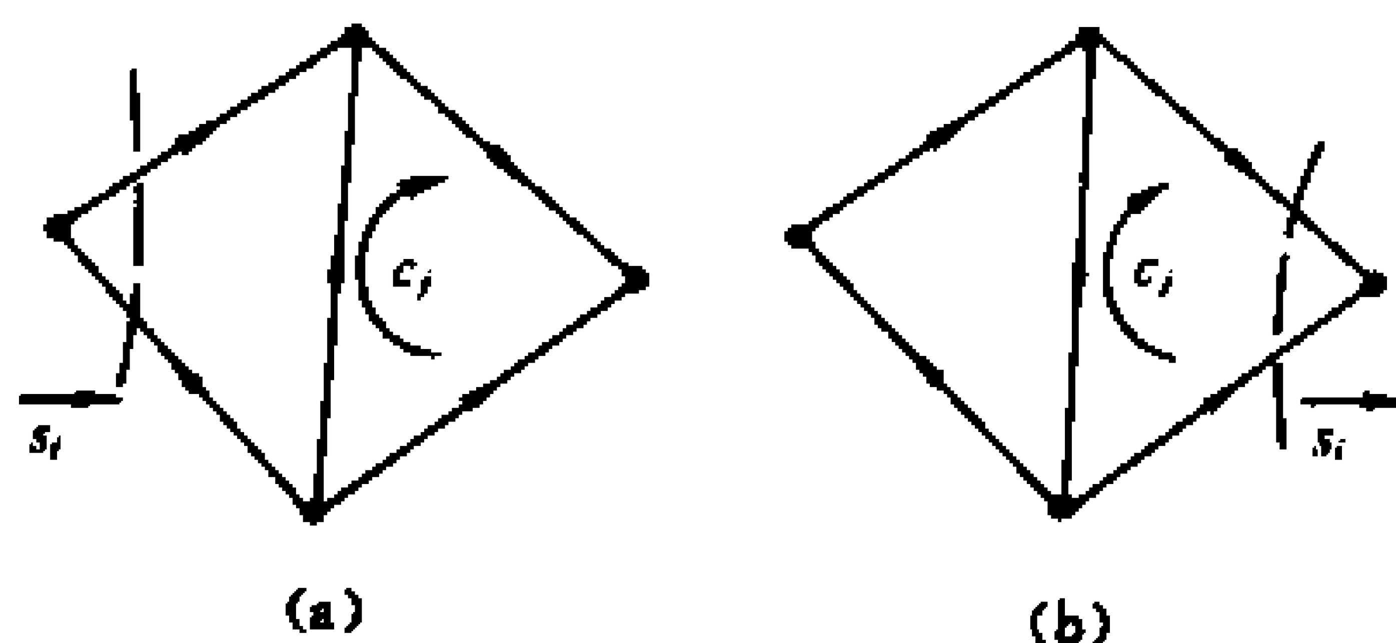


图 3.15

1. S_i 与 C_j 不相交，即 C_j 中的边在 S_i 里不出现，自然 $d_{ij}=0$。

2. S_i 与 C_j 相交，显然它们有偶数条共同的边，如图 3.15(b)所示，其中相邻两条边 e_p, e_q 组成一对，如果它们在 S_i 中方向一致，则在 C_j 中方向相反，反之亦然。因此 $d_{ij}=0$。

由 d_{ij} 的任意性，定理得证。

定理 3.4.6 连通图 G 的完全割集矩阵 S_e 的秩是 $n-1$。

证明：由于 S_f 是 S_e 的子矩阵，而 ran $S_f=n-1$，因此 ran $S_e\geqslant n-1$。又由定理3.4.5，$S_eC_e^T=0$，根据 sylvester 定理，ran S_e+ran $C_e\leqslant m$，故 ran $S_e\leqslant n-1$。因此 ran $S_e=n-1$。

定义 3.4.8 连通图 G 的 $n-1$ 个互相独立的割集构成的矩阵称为 G 的割集矩阵。记为 S。

割集矩阵 S 有以下简单性质

1. 基本割集矩阵 S_f 是割集矩阵。

2. $SC^T=0$ S 和 C 的边次序一致。

3. $S=PS_f$ 其中 P 是非奇异方阵，S 与 S_f 的边次序一致。

定理 3.4.7 连通图 $G=(V,E)$ 的割集矩阵 S 的任一 $n-1$ 阶子阵行列式非零，当且仅当这些列对应于 G 的某棵树。

证明：充分性。设已知 G 的某棵树 T，则可构造基本割集矩阵 $S_f=(S_{f_{11}}\ \ I)$。对给定的割集矩阵 S 进行列交换，使其与 S_f 的边次序一致，于是可写成分块矩阵形式 $S=(S_{11}\ S_{12})$，其中 S_{12} 对应树 T。由性质 3，$S=PS_f$，即 $(S_{11}\ S_{12})=P(S_{f_{11}}\ I)=(PS_{f_{11}}\ P)$。因此 $S_{12}=P$，是非奇异的，即其行列式非零。必要性。调整 S 的这 $n-1$ 列构成 S_{12}，使 $S=(S_{11}\ S_{12})$。假定 S_{12} 的各列对应的不是树，则一定含有 $l(<n)$ 条边的初级回路 C。由于 C 是 G 的连通子图，因此 C 的割集矩阵的秩是 $l-1$，亦即 S_{12} 对应的这 l 列线性相关，故 $|S_{12}|=0$，矛盾。

定理 3.4.8 设 S_f 和 C_f 分别是连通图 G 中关于某棵树 T 的基本割集矩阵和基本回路矩阵，且边次序一致。并设 $S_f=(S_{f_{11}}\ I)$，$C_f=(I\ C_{f_{12}})$，则 $S_{f_{11}}=-C_{f_{12}}^T$。

证明：由定理 3.4.5，有

$$S_fC_f^T=0。$$

$$(S_{f_{11}}\ I)\begin{bmatrix}I\\C_{f_{12}}^T\end{bmatrix}=0,$$

故得证。

推论 3.4.1 当连通图 G 的基本割集矩阵与基本关联矩阵的边次序一致时，有

$$S_{f_{11}}=B_{12}^{-1}B_{11}。$$

例 3.4.7 已知图 3.15 的基本关联矩阵

$$B_1=\begin{bmatrix}-1&0&0&-1&0&1\\0&1&0&1&1&0\\0&0&-1&0&-1&-1\end{bmatrix}$$
$$\begin{matrix}e_1&e_2&e_3&e_4&e_5&e_6\end{matrix}$$

其中 $\{e_2,e_3,e_4\}$ 构成 G 的树，求对应的基本割集矩阵。

解：对 B_1 的列重新调整如下

$$B_1=\begin{bmatrix}-1&0&1&0&0&-1\\0&1&0&1&0&1\\0&-1&-1&0&-1&0\end{bmatrix}$$
$$\begin{matrix}e_1&e_5&e_6&e_2&e_3&e_4\end{matrix}$$

$$B_{11}=\begin{bmatrix}-1 & 0 & 1\\ 0 & 1 & 0\\ 0 & -1 & -1\end{bmatrix}\quad B_{12}=\begin{bmatrix}0 & 0 & -1\\ 1 & 0 & 1\\ 0 & -1 & 0\end{bmatrix}\quad B_{12}^{-1}=\begin{bmatrix}1 & 1 & 0\\ 0 & 0 & -1\\ -1 & 0 & 0\end{bmatrix}$$

$$\therefore\qquad S_f=(B_{12}^{-1}B_{11}\quad I)=\begin{bmatrix}-1 & 1 & 1 & 1 & 0 & 0\\ 0 & 1 & 1 & 0 & 1 & 0\\ 1 & 0 & -1 & 0 & 0 & 1\end{bmatrix}$$

$$\qquad\qquad\qquad\qquad e_1\quad e_5\quad e_6\quad e_2\quad e_3\quad e_4$$

3.5 支撑树的生成

在 3.3 节中我们讨论了连通图树的计数方法，其计算过程十分方便。不过它还不能给出每棵树的具体构成。但在有些场合这又恰恰是十分需要的。本节介绍 Mayeda 等提出的利用基本树变换生成 G 的全部支撑树的算法，该算法与基本割集有紧密联系。先介绍一些有关知识。

为方便起见，本节中用 t 表示 G 的一棵树。假定 t_1,t_2 是连通图 G 的两棵树，t_1 中共有 k 条边不属于 t_2，则称 t_1 和 t_2 的距离 $d(t_1,t_2)=k$。当然，此时也有 $d(t_2,t_1)=k$。

定义 3.5.1 设 t_1,t_2 是连通图 G 距离为 1 的两棵树。$t_1-t_2=(e)$，$t_2-t_1=(e')$。则 $t_2=t_1\oplus(e,e')$ 称为 t_1 到 t_2 的基本树变换。

由于 $e'\notin t_1$，因此它是 t_1 的一条余树边。$t_1+(e')$ 含有一条唯一回路 C，$e\in C$。所以 $t_1\oplus(e,e')$ 又形成了 G 的另一棵树 t_2。

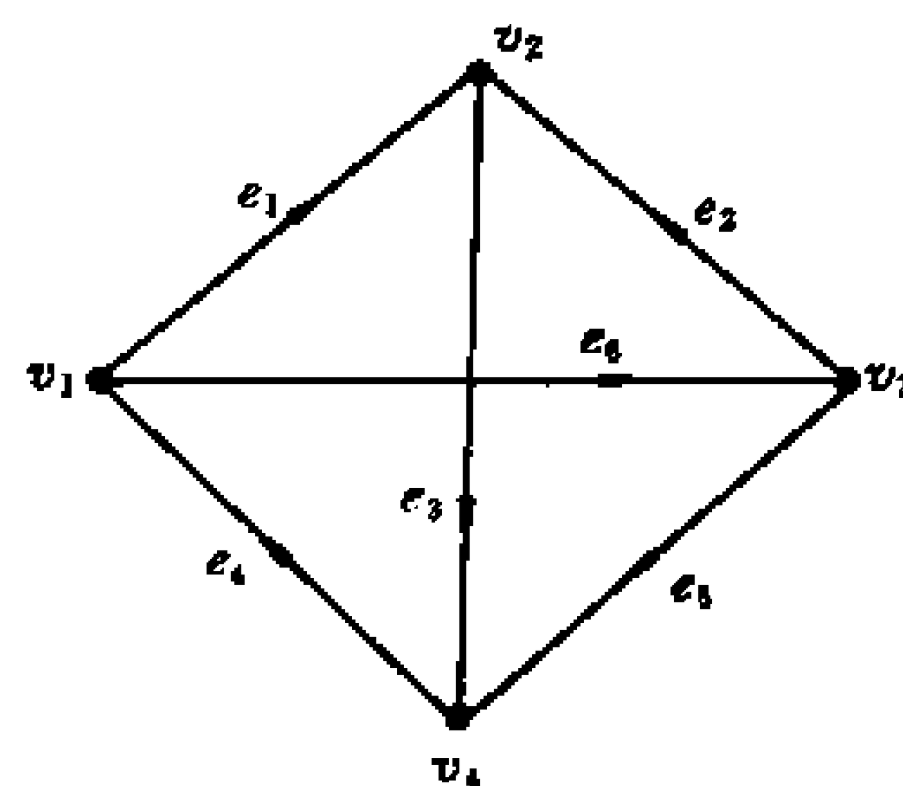


图 3.16

例 3.5.1 图 3.16 中，设 $t_1=(e_2,e_3,e_4)$，$t_2=(e_2,e_3,e_6)$，则 $t_2=t_1\oplus(e_4,e_6)$ 是 t_1 到 t_2 的基本树变换。

给定 G 的一棵树 t_0，就可以得到 $n-1$ 个基本割集 $s_{e_i}(t_0)$，它们的集合叫基本割集组，记作 S。其中每一个基本割集 $s_{e_i}(t_0)$ 都对应 t_0 中唯一的一条树枝 e_i。比如在图 3.16中，令 $t_0=(e_1,e_2,e_3)$，有

$$s_{e_1}(t_0)=(e_1,e_4,e_6),\ s_{e_2}(t_0)=(e_2,e_5,e_6),\ s_{e_3}(t_0)=(e_3,e_4,e_5)。$$

假定基本割集 $s_e(t_1)=(e,a_1,a_2,\cdots,a_k)$，且 t_2 是不含 e 且与 t_1 距离为 1 的另一棵树。令 $t_2-t_1=(b)$，那么边 b 有什么特点呢?

定理 3.5.1 令 t_1,t_2 是 G 中距离为 1 的两棵树，且 $t_1-t_2=(e)$，$t_2-t_1=(b)$，则 $b\in s_e(t_1)$。反之若 $b\in s_e(t_1)$，则 $t_1\oplus(e,b)$ 是树。

证明：由 $t_1-t_2=(e)$，$t_2-t_1=(b)$，可得 $t_1\oplus t_2=(e,b)$。

设 $t_1=(e,a_1,a_2,\cdots,a_k)$。

$t_2=(b,a_1,a_2,\cdots,a_k)$。

若 $b\notin s_e(t_1)$，由于 $s_e(t_1)$ 不含 t_1 其它树枝边 $a_1,a_2,\cdots,a_k$，故 $s_e(t_1)$ 不含 t_2 的任一条边。这样删去 $s_e(t_1)$ 的全部边之后，t_2，亦即 G 仍连通，这与 $s_e(t_1)$ 是割集矛盾。

反之，若 $b\in s_e(t_1)$，而 $s_e(t_1)$ 只含 t_1 的唯一树枝 e。因此 $b\neq a_i(i=1,2,\cdots,k)$，所以 $b\notin t_1$。t_1+b 存在含 e 的唯一回路，因此 $t_1\oplus(e,b)$ 连通，同时有 $n-1$ 条边。它是一棵树。

由于 $s_e(t_1)$ 中的边 b 是任意的，所以立即可以进行推广。

定理 3.5.2 给定 G 的一棵树 t_0，令 $t_1,t_2,\cdots,t_p$ 是 G 中全部满足

$$\begin{aligned} t_0-t_i&=(e), \\ t_i-t_0&=(b_i), \end{aligned} \qquad i=1,2,\cdots,p。$$

的树，则 $s_e(t_0)=(e,b_1,b_2,\cdots,b_p)$。反之若 $b_i\in s_e(t_0)$，则 $t_i=t_0\oplus(e,b_i)$ 是树。

例 3.5.2 在图 3.16 中，令 $t_0=(e_1,e_2,e_3)$。则 $t_1=(e_4,e_2,e_3)$，$t_2=(e_6,e_2,e_3)$，满足 $t_0-t_1=(e_1)$，$t_1-t_0=(e_4)$，$t_2-t_0=(e_6)$，$s_{e_1}(t_0)=(e_1,e_4,e_6)$。

例 3.5.3 图 3.16 中令 $t_0=(e_1,e_2,e_3)$。每个树枝所对应的基本割集是

$$s_{e_1}(t_0)=(e_1,e_4,e_6)。$$

$$s_{e_2}(t_0)=(e_2,e_5,e_6)。$$

$$s_{e_3}(t_0)=(e_3,e_4,e_5)。$$

因此 G 中与 t_0 距离为 1 的全部树是

由 $s_{e_1}(t_0)$

$$t_1=(e_4,e_2,e_3)。$$

$$t_2=(e_6,e_2,e_3)。$$

由 $s_{e_2}(t_0)$

$$t_3=(e_1,e_5,e_3)。$$

$$t_4=(e_1,e_6,e_3)。$$

由 $s_{e_3}(t_0)$

$$t_5=(e_1,e_2,e_4)。$$

$$t_6=(e_1,e_2,e_5)。$$

这样可以定义这些树的集合。

定义 3.5.2 令

$$T^e=\{t_0\oplus(e,b)\mid b\in s_e(t_0),b\neq e\}。$$

T^e 表示对 G 的某棵参考树 t_0，$e\in t_0$。逐一用其基本割集 $s_e(t_0)$ 的每条边去替换 e，即进行基本树变换之后的新树集合。

对于上例，可得 $T^{e_1}=\{t_1,t_2\}$，$T^{e_2}=\{t_3,t_4\}$，$T^{e_3}=\{t_5,t_6\}$。采用这种符号表示之后，我们有

定理 3.5.3 设 $t_0=(e_1,e_2,\cdots,e_k)$ 是 G 中的参考树。则 G 中与 t_0 距离为 1 的树恰在

$$T^{e_1},T^{e_2},\cdots,T^{e_k}$$

的某个集合之中。

证明：其存在性正是定理 3.5.2 的推广。现证其唯一性。由于 T^{e_i} 中的每棵树 t 都是由基本割集 $s_{e_i}(t_0)$ 中的某条边替代 t_0 中的 e_i 而得，t 中不可能有 e_i。反之，因为 $t\in T^{e_i}$，它与 t_0 的距离为 1。就是说 t_0 除边 e_i 之外，其余各边都属于 t。所以若 $e_i\in t_0$，$e_j\in t_0$，$e_i\neq e_j$。则对 T^{e_i} 中的每棵树 t，$e_i\notin t$ 而 $e_j\in t$，而对 T^{e_j} 的每棵树 t'，$e_j\notin t'$ 而 $e_i\in t$。显见 $T^{e_i}\bigcap\limits_{i\neq j}T^{e_j}=\Phi$。

类似的方法，令

$$T^{e_r e_s} = \{t \oplus (e_s, b) \mid b \in S_{e_s}(t),\ t \in T^{e_r}, b \neq e_s\}。$$

对参考树 t_0 中的一条树边 e_r，先求替换 e_r 的与 t_0 距离为 1 的树的集合 T^{e_r}，然后对 T^{e_r} 中的每棵树 t，若 e_s 是它们的树枝，再进行一次基本树变换。即用 e_s 所对应的以 t 为树的基本割集中的其余边 b 来替换 e_s。从而得到 $T^{e_r e_s}$ 中的一棵树。

例 3.5.4 令 $t_0=(e_1,e_2,e_3)$ 是图 3.16 的参考树。则 $T^{e_1}=\{(e_4,e_2,e_3),(e_6,e_2,e_3)\}$，其中 $t_1=(e_4,e_2,e_3)$，$t_2=(e_6,e_2,e_3)$。这时

$$s_{e_2}(t_1) = (e_2,e_5,e_6), s_{e_2}(t_2) = (e_2,e_1,e_4,e_5),$$

于是由 $s_{e_2}(t_1)$ 得到

$$t_1' = (e_5,e_4,e_3)。$$

$$t_2' = (e_6,e_4,e_3)。$$

由 $s_{e_2}(t_2)$ 得到

$$t_3' = (e_1,e_6,e_3)。$$

$$t_4' = (e_4,e_6,e_3)。$$

$$t_5' = (e_5,e_6,e_3)。$$

从中发现，t_3' 就是例 3.5.3 中的 t_4，即它与 t_0 的距离为 1。而其余树虽然都与 t_0 的距离为 2，但 t_2' 与 t_4' 是同一棵树，计算重复。首先解决前一个问题。

定义 3.5.3 设 $t_0=(e_1,e_2,\cdots,e_{n-1})$ 是 G 的一棵参考树。定义

$$T^{e_1e_2} = \{t \oplus (e_2,b) \mid b \in s_{e_2}(t) \cap s_{e_2}(t_0), t \in T^{e_1}, b \neq e_2\}。$$

比如上例中

$$s_{e_2}(t_1) \cap s_{e_2}(t_0) = (e_2,e_5,e_6) \cap (e_2,e_5,e_6) = (e_2,e_5,e_6)。$$

$$s_{e_2}(t_2) \cap s_{e_2}(t_0) = (e_2,e_1,e_4,e_5) \cap (e_2,e_5,e_6) = (e_2,e_6)。$$

因此只有 t_1'，t_2' 和 t_5' 属于 $T^{e_1e_2}$。

由于 $s_{e_2}(t_0)$ 是图 G 关于树 t_0 的包含树枝 e_2 的基本割集。由于 e_1，e_2 都在 t_0 中，所以割集 $s_{e_2}(t_0)$ 不会包含另一条树枝 e_1，即 $e_1 \notin s_{e_2}(t) \cap s_{e_2}(t_0)$，当然 $e_2 \notin s_{e_2}(t) \cap s_{e_2}(t_0)$。即 $T^{e_1e_2}$ 中的每棵树包含了 t_0 中除 e_1，e_2 之外的所有边，并对任意 $t \in T^{e_1e_2}$，都有 $d(t,t_0)=2$。因此可以得到结论

定理 3.5.4 与 $t_0=(e_1,e_2,\cdots,e_{n-1})$ 距离为 2 的全部支撑树都在集合 $T^{e_ie_j}$ 之中，e_i，$e_j \in t_0$，$i \neq j$。

一般情况下，可以定义 $T^{e_1e_2\cdots e_k}$ 如下

$$T^{e_1e_2\cdots e_k} = \{t \oplus (e_k,b) \mid b \in s_{e_k}(t) \cap s_{e_k}(t_0),$$

$$t \in T^{e_1e_2\cdots e_{k-1}}, b \neq e_k, k < n\}。$$

这样，如果令 $T^1=\bigcup T^{e_i}$，$e_i \in t_0$。$T^2=\bigcup T^{e_ie_j}$，$e_i,e_j \in t_0$，$\cdots$。$T_k=\bigcup T^{e_{i1}e_{i2}\cdots e_{ik}}$，$e_{ij} \in t_0$，$j=1,2,\cdots,k$。就可以得到

定理 3.5.5 设 t_0 是连通图 G 的参考树，$t \neq t_0$ 是 G 的任一棵支撑树，那么一定有 $t \in \bigcup_{i=1}^{n-1} T^i$。

证明：设 $d(t-t_0)=l(1\leqslant l\leqslant n-1)$，即 t_0 中必有 l 条边不属于 t。不妨设它们是 $e_1,e_2,\cdots,e_l$。由 $T^{e_1e_2\cdots e_l}$ 定义即得 $t\in T^l$。

综上我们可以给出连通图 G 全部生成树的生成算法。

a. 给定参考树 t_0，$T_0\leftarrow\{t_0\}$，$j\leftarrow 1$。

b. 计算 T^j，$T_0\leftarrow T_0\cup T^j$。

c. $j\leftarrow j+1$，若 $j<n$，执行 b，否则结束。

算法结束时，T_0 包含了 G 的全部树。其中步骤 b 最为复杂，它要分 C_{n-1}^j 种情况计算 $T^{e_{i_1}e_{i_2}e_{i_j}}$。在步骤 b 第 j 次迭代时，与 t_0 距离为 j 的树都会得到，而任何距离小于 j 的树都不会出现，因此该算法是较好的。但是它并没有保证对每一棵与 t_0 距离为 j 的树 t，只在 C_{n-1}^j 种情况之一出现。关于这一点，Mayeda 等给出了解决办法，这里就不再讨论。

最后，仍以图 3.16 为例，给出该算法的一个完整过程。

例 3.5.5 以 $t_0=(e_1,e_2,e_3)$ 为参考树，求 G 的全部生成树。

解：由前面诸例已得

1. $T^0=\{t_0\}=\{(e_1,e_2,e_3)\}$。

2. $T^1=T^{e_1}\cup T^{e_2}\cup T^{e_3}=\{(e_4,e_2,e_3),(e_6,e_2,e_3)\}\cup\{(e_1,e_5,e_3),(e_1,e_6,e_3)\}\cup\{(e_1,e_2,e_4),(e_1,e_2,e_5)\}$。

   其中 $s_{e_1}(t_0)=(e_1,e_4,e_6)$，$s_{e_2}(t_0)=(e_2,e_5,e_6)$，$s_{e_3}(t_0)=(e_3,e_4,e_5)$。

3. $T^2=T^{e_1e_2}\cup T^{e_1e_3}\cup T^{e_2e_3}$。

   (a) 其中 $T^{e_1e_2}=\{(e_5,e_4,e_3),(e_6,e_4,e_3),(e_5,e_6,e_3)\}$。

   (b) 计算 $T^{e_1e_3}$。其中 T^{e_1} 包括 $t_1=(e_4,e_2,e_3)$，$t_2=(e_6,e_2,e_3)$，于是

$$s_{e_3}(t_1)\cap s_{e_3}(t_0)=(e_1,e_3,e_5,e_6)\cap(e_3,e_4,e_5)=(e_3,e_5)。$$

$$s_{e_3}(t_2)\cap s_{e_3}(t_0)=(e_3,e_4,e_5)\cap(e_3,e_4,e_5)=(e_3,e_4,e_5)。$$

$$T^{e_1e_3}=\{(e_5,e_4,e_2),(e_4,e_6,e_2),(e_5,e_6,e_2)\}。$$

   (c) 计算 $T^{e_2e_3}$。其中 T^{e_2} 包括 $t_1=(e_3,e_1,e_5)$，$t_2=(e_3,e_1,e_6)$，这样

$$s_{e_3}(t_1)\cap s_{e_3}(t_0)=(e_3,e_2,e_4,e_6)\cap(e_3,e_4,e_5)=(e_3,e_4)。$$

$$s_{e_3}(t_2)\cap s_{e_3}(t_0)=(e_3,e_4,e_5)\cap(e_3,e_4,e_5)=(e_3,e_4,e_5)。$$

$$T^{e_2e_3}=\{(e_4,e_1,e_5);(e_4,e_1,e_6),(e_5,e_1,e_6)\}。$$

∴ T^2 包括了 9 棵树。

4. 计算 $T^3=T^{e_1e_2e_3}$

由 $T^{e_1e_2}=\{(e_3,e_4,e_5),(e_6,e_4,e_3),(e_5,e_6,e_3)\}$ 可得

$$s_{e_3}(t'_1)\cap s_{e_3}(t_0)=(e_1,e_2,e_3)\cap(e_3,e_4,e_5)=(e_3)。$$

$$s_{e_3}(t'_2)\cap s_{e_3}(t_0)=(e_1,e_2,e_3)\cap(e_3,e_4,e_5)=(e_3)。$$

$$s_{e_3}(t'_3)\cap s_{e_3}(t_0)=(e_1,e_2,e_3)\cap(e_3,e_4,e_5)=(e_3)。$$

故

$$T^3=\Phi.$$

因此最终共有 16 棵不同的树，如图 3.17 所示。

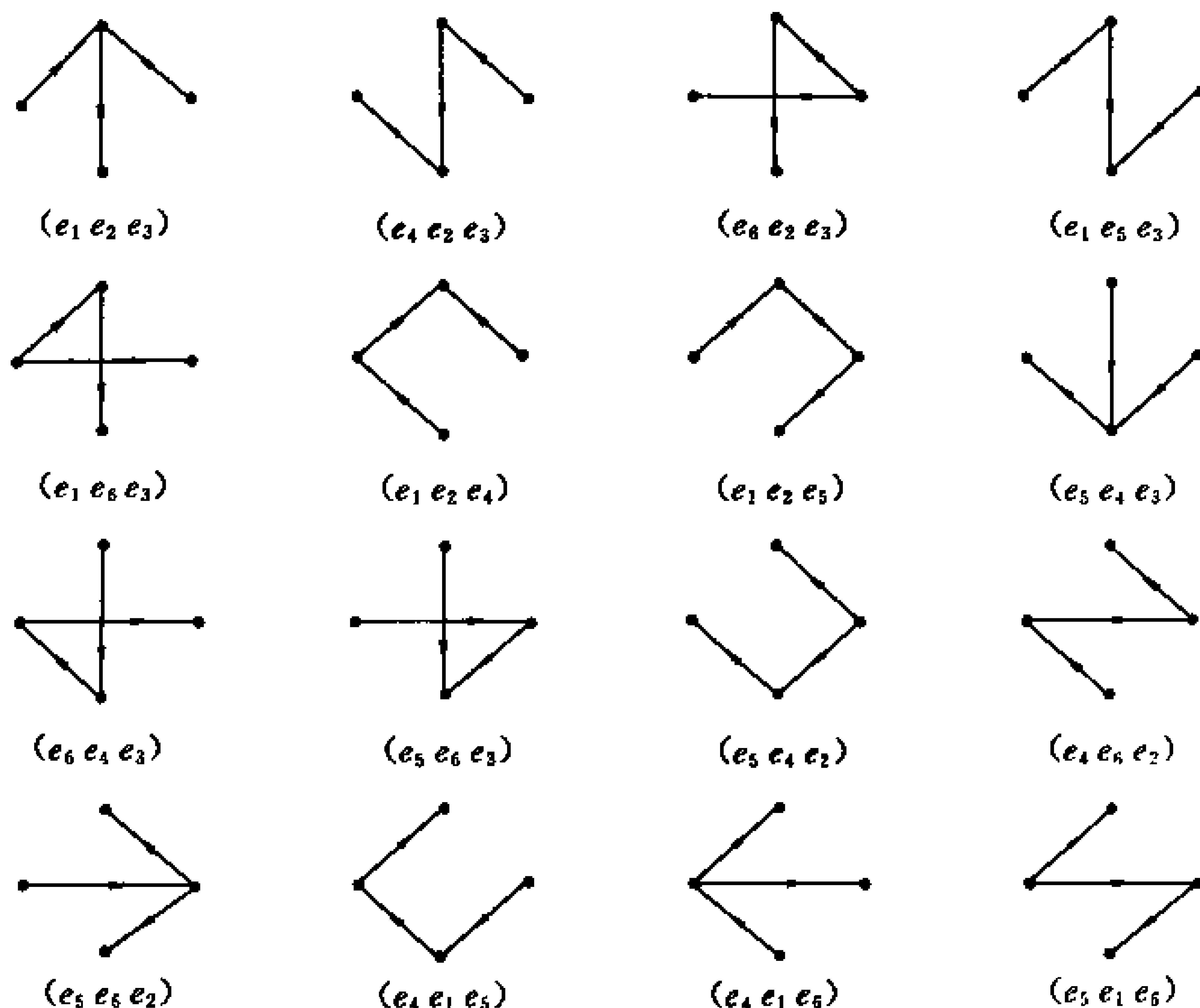


图 3.17

Mayeda 算法的关键在步骤 b。每进行一次基本树变换，就需要计算 $S_e(t)$。设 $e=(u,v)$，则 $t-e$ 中 u 与 v 分属两个不同连通支：$G_1=(V_1,E_1)$，$G_2=(V_2,E_2)$。这时 G 中两端点分别在 V_1 和 V_2 的边 $b\in S_e(t)$。因此求基本割集的计算复杂度为 $O(m)$。如果 G 中有 p 棵树，则该算法最坏情况下，其计算复杂性是 $O(pm)$。

3.6 Huffman 树

以下三节讨论树的应用，首先介绍最优二叉树。

定义 3.6.1 除树叶外，其余结点的正度最多为 2 的外向树称为二叉树。如果它们的正度都是 2，称为完全二叉树。

例如图 3.18 是一棵完全二叉树，v_0 是根，每条有向边的方向都是朝下的。如果二叉树 T 的每个树叶结点 v_i 都分别赋以一个正实数 w_i，则称 T 是赋权二叉树。从根到树叶 v_i 的路径 $P(v_0,v_i)$ 所包含的边数计为该路径的长度 l_i，这样二叉树 T 带权的路径总长是

$$\text{WPL} = \sum_i l_i w_i,\quad v_i \text{ 是树叶。}$$

反过来，如果给定了树叶数目以及它们的权值，可以构造许多不同的赋权二叉树。在这些赋权二叉树中，必定存在路径总长最小的二叉树，这样的树称为最优二叉树。

例 3.6.1 已知英文字符串 adacatedecade。试用二进制字符串代替某个字母，并保证

该英文字符串与二进制串构成一一对应。

解：该字符串中有字母 a,d,e,c,t，它们分别出现 4，3，3，2，1 次。令每个字母对应二叉树的一个树叶，根到树叶的路径是唯一的，而且这条路径决不会是根到另一个树叶路径的一部分。这样根到树叶的路径与该字母构成一一对应。如果在树 T 中令向左的边为 0，向右的边为 1。那么这些路径又与二进制串构成了一一对应。

例如令 d,a,e,c,t 分别对应图 3.18 的 v_3,v_5,v_6,v_7,v_8，则 $d\leftarrow 00$，$a\leftarrow 010$，$e\leftarrow 011$，$c\leftarrow 10$，$t\leftarrow 11$。该英文字符串对应 0100001010010101100011100100001l。

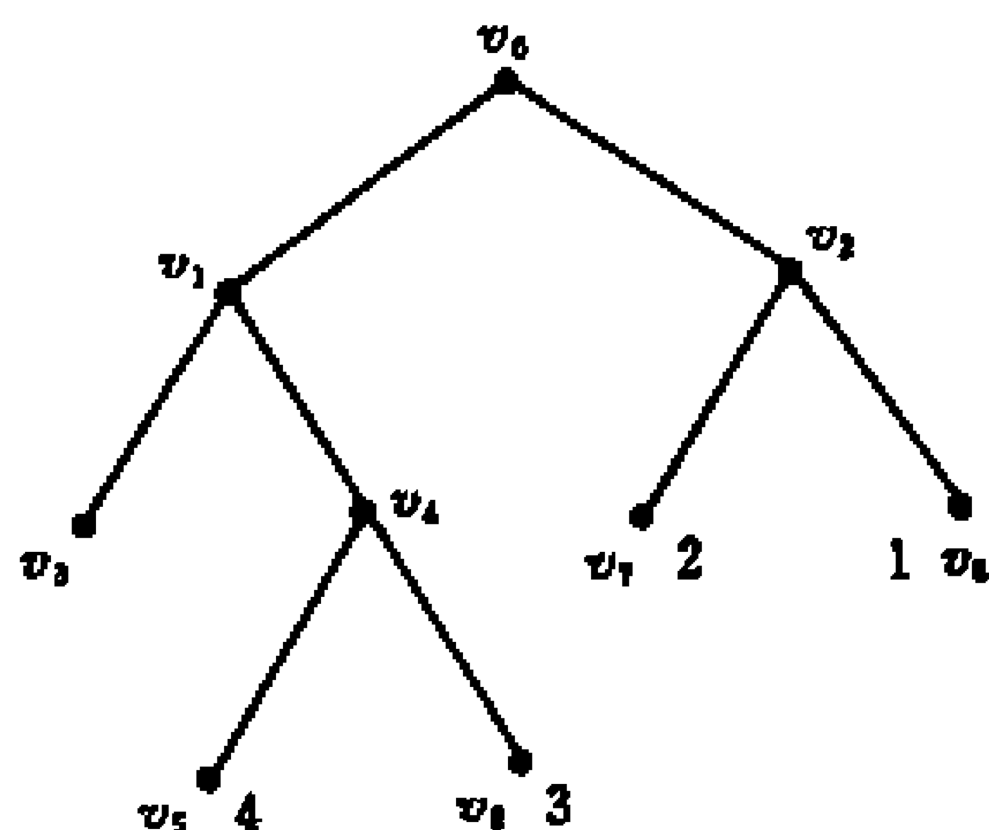


图 3.18

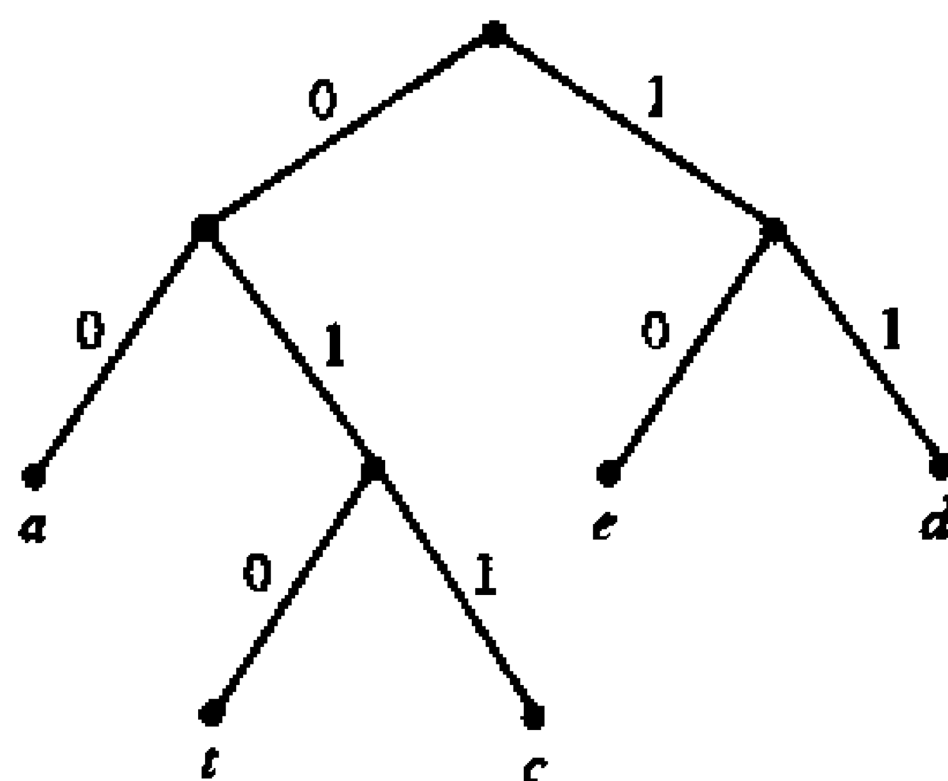


图 3.19

如果字母与树叶的对应情况如图 3.19 所示。即 $a\leftarrow 00$，$t\leftarrow 010$，$c\leftarrow 011$，$e\leftarrow 10$，$d\leftarrow 11$。则对应字符串是 00110001100010101110011001110。这两种情况下字符串的总长分别是 33 和 29。

给定了 n 个树叶的权值，如何构造带权路径总长最短的最优二叉树呢？哈夫曼给出了一个算法。由该算法得到的二叉树称为 Huffman 树。

算法描述如下：

a. 对 $n(\geqslant 2)$ 个权值进行排序，满足

$$w_{i_1}\leqslant w_{i_2}\leqslant\cdots\leqslant w_{i_n}。$$

b. 计算 $w_i=w_{i_1}+w_{i_2}$ 作为中间结点 v_i 的权，v_i 的左儿子是 v_{i_1}，右儿子是 v_{i_2}。在权序列中删去 w_{i_1},w_{i_2}，加入 w_i，$n\leftarrow n-1$。若 $n=1$，结束。否则转 a。

例 3.6.2 权序列为(4，3，3，2，1)的 Huffman 树的构造过程是：

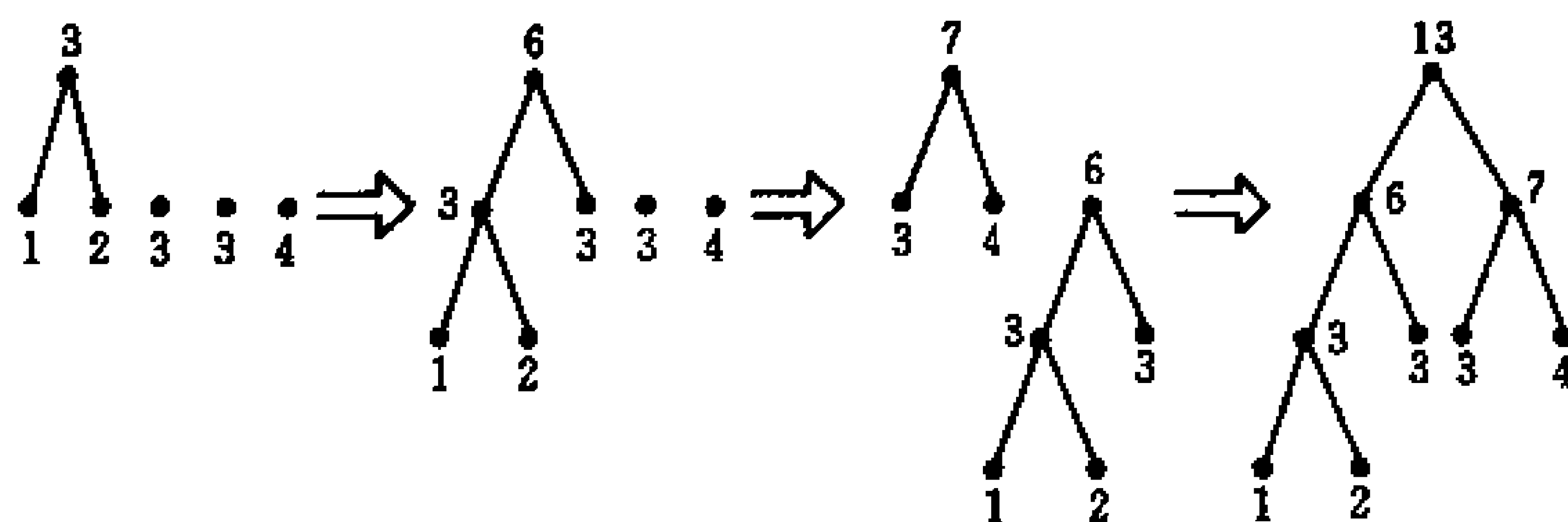


图 3.20

算法的计算复杂度主要取决于步骤 a，而且是 n 个权值的第一次排序，它一般需进行 $n\log n$ 次比较。之后每当产生 w_i 时，只需在新序列中进行插入运算，其复杂性是 $\log n$，由

于总共只进行 $n-2$ 次迭代，因此整个算法的计算复杂性是 $O(n\log n)$。

定理 3.6.1 由 Huffman 算法得到的二叉树是最优二叉树。

证明：假定 $n\geqslant 3, w_1\leqslant w_2\leqslant\cdots\leqslant w_n$，并设 T 是最优树。则一定有 $l_1=\max\limits_i\{l_i\}$。否则，若 $w_k>w_1$ 而 $l_k<l_1$。那么将 w_k 与 w_1 对调得到 T'。有 $\mathrm{WPL}(T')-\mathrm{WPL}(T)<0$，与 T 最优矛盾。于是可得到结论：只要 T 是最优树，w_1 就一定离根最远。同时立即可知，w_1 必有兄弟。否则让 w_1 赋值给该树叶的父亲结点，就可得到路径总长更小的树。由于 w_2 是序列中次最小的权，故可令 w_1 的兄弟是 w_2。因此分枝 w_1+w_2（如图 3.21）可以是最优树 T 的子图。

设 T_n 是 n 个树叶的最优树，收缩分支 w_1+w_2 后是对应的 $n-1$ 个树叶的 T'_{n-1}，如图 3.22 所示。

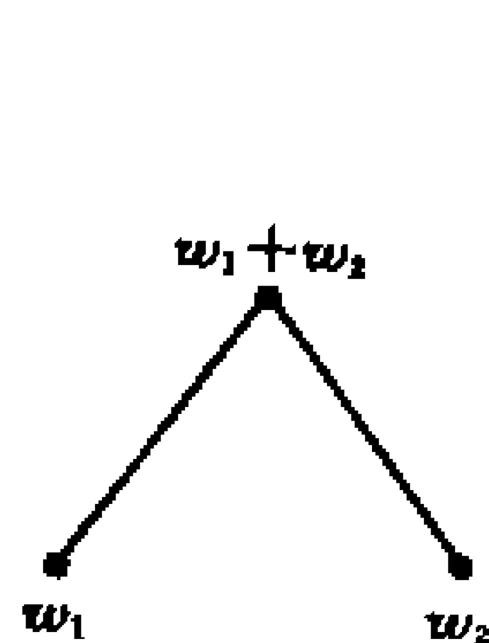


图 3.21

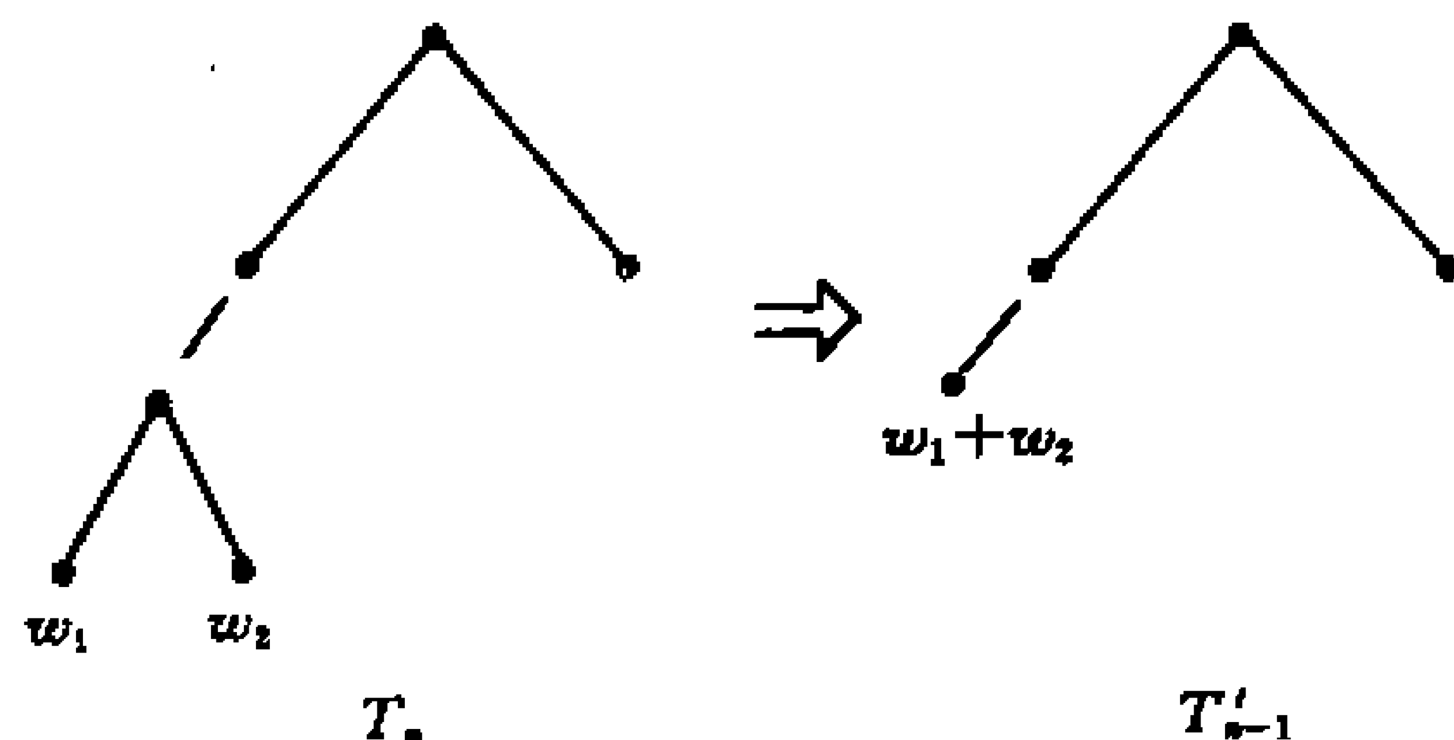


图 3.22

在 $n-1$ 个权（其中之一是 w_1+w_2）时，亦有其最优二叉树 T_{n-1}，然后将 w_1+w_2 分支展开后又得到有 n 个权的二叉树 T'_n，如图 3.23 所示

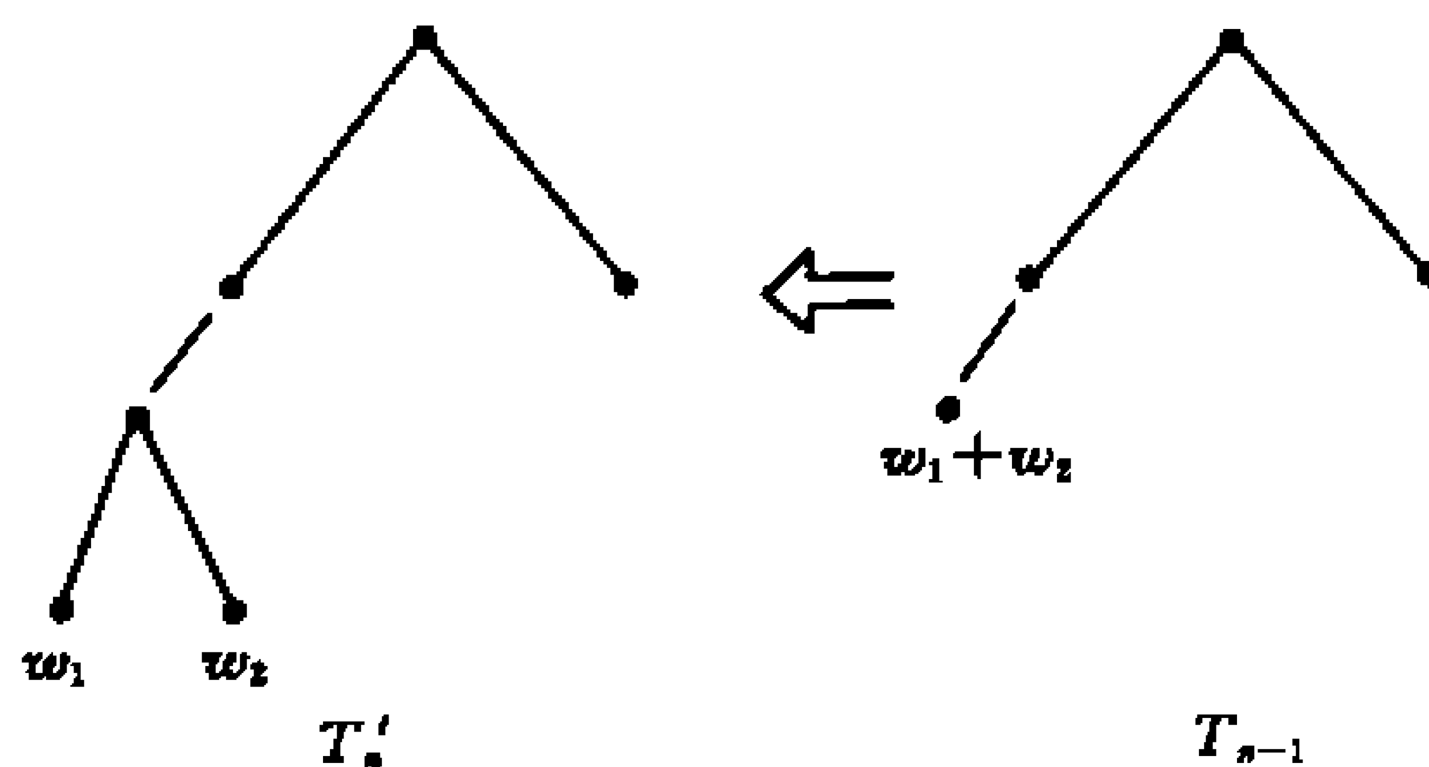


图 2.23

因为 T_n 和 T_{n-1} 分别是最优树，所以 $\mathrm{WPL}(T_n)\leqslant\mathrm{WPL}(T'_n)$，$\mathrm{WPL}(T_{n-1})\leqslant\mathrm{WPL}(T'_{n-1})$。由于

$$\mathrm{WPL}(T'_{n-1}) = \mathrm{WPL}(T_n) - (w_1 + w_2),$$
$$\mathrm{WPL}(T_{n-1}) = \mathrm{WPL}(T'_n) - (w_1 + w_2),$$

可得 $\mathrm{WPL}(T'_{n-1})\leqslant\mathrm{WPL}(T_{n-1})$。亦即 T'_{n-1}, T'_n 都是最优树。

当算法执行到 $n=2$ 时，自然是一棵最优树。再与分枝收缩的过程相反进行展开，最后得到的 T'_n 一定是最优二叉树。

3.7 最 短 树

在赋权连通图中，有时需要计算其总长最小或最大的支撑树。这就是最短树和最长树问题。例如要在若干加油站之间铺设输油管道，已知任意两个加油站之间输油管道的铺设费用，如果让每个站都能保证油的供应，那么最少的建造费用就应该是计算它的最短树。

以下介绍关于赋权连通图 G 最短树的两个好算法。它们分别是由 Kruskal 和 Prim 提出来的。

3.7.1 Kruskal 算法

Kruskal 算法的描述如下：

$T \leftarrow \Phi$。

当 $|T|<n-1$ 且 $E\neq\Phi$ 时，

begin

a. $e\leftarrow E$ 中最短边。

b. $E\leftarrow E-e$。

c. 若 $T+e$ 无回路，则 $T\leftarrow T+e$。

end。

若 $|T|<n-1$ 打印"非连通"，否则输出最短树。

该算法的思路是不断往 T 中加入当前的最短边 e，如果此时会构成回路，那么它一定是这个回路中的最长边，删之。直至最后达到 $n-1$ 条边为止。这时 T 中不包含任何回路，因此是树。

例 3.7.1 对图 3.24 执行 Kruskal 算法的过程是 $T\leftarrow(v_4,v_3),(v_4,v_5),(v_1,v_2)$。当加入 (v_3,v_5) 时会构成回路，因此边 (v_3,v_5) 不加入 T。此后 $T\leftarrow T+(v_2,v_4)$。这时 $|T|=n-1$，$T=\{(v_4,v_3),(v_4,v_5),(v_1,v_2),(v_2,v_4)\}$，结束。

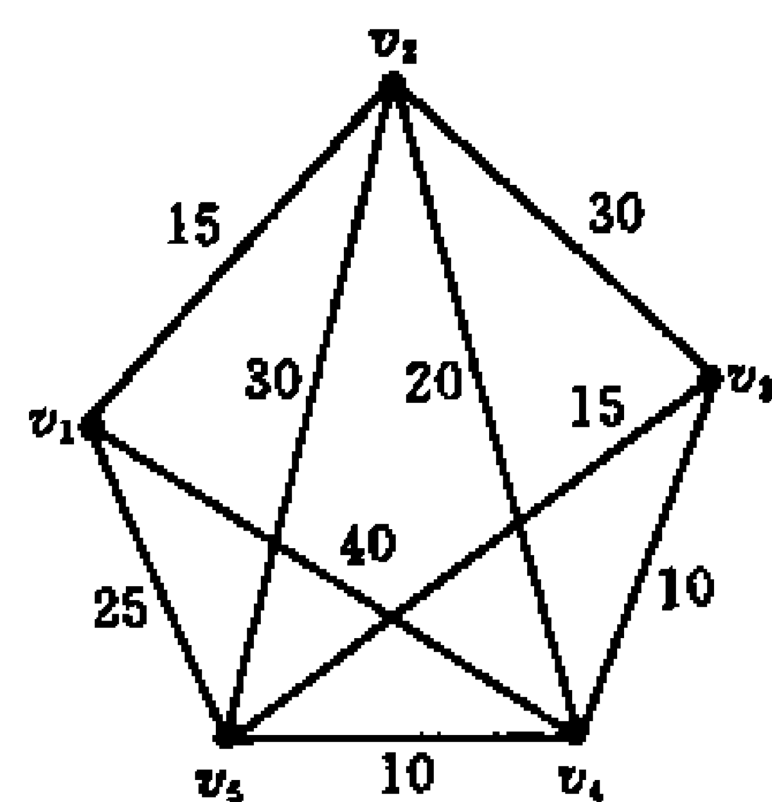


图 3.24

定理 3.7.1 $T=(V,E')$ 是赋权连通图 $G=(V,E)$ 的最短树，当且仅当对任意的余树边 $e\in E-E'$，回路 $C^e(C^e\subseteq E'+e)$ 满足其边权

$$w(e)\geqslant w(a),\ a\in C^e(a\neq e)。$$

证明：必要性。如果存在一条余树边 e，满足 $w(e)<w(a)$，$a\in C^e$，则 $T\oplus(a,e)$ 得到新树 T' 比 T 更短，与 T 是最短树矛盾。再证充分性。若存在比 T 还短的树 T'，则 $T'-T\neq\Phi$，设 $e\in T'-T$，则 $T+e$ 构成唯一回路 C^e。如果对任意的 T' 关于 T 的余树边 $e\in T'-T$，它与回路 C^e 里的树枝边 a $(a\in C^e\cap T)$ 相比都有 $w(e)\geqslant w(a)$，则有 $w(T')\geqslant w(T)$，与假设矛盾。因此一定存在某边 $e\in T'-T$，对于某条边 $a\in C^e\cap T$，满足 $w(e)<w(a)$。

定理保证了 Kruskal 算法的正确性。以下讨论它的计算复杂性。很显然，在迭代过程中复杂度主要取决于步骤 a 和 c。

对 m 条边的权采用堆结构存放，可以保证根结点是当前的最小权。堆结构是一种均衡二叉树，它满足对任何一个父亲结点，其权都小于等于其左、右儿子的权。初始，构造一个有 m 个结点的均衡二叉树，每一个结点的权对应原赋权图 G 中一条边的权。一般它不满足堆结构的排序要求，所以首先要建堆。比如对图 3.25(a)的二叉树，最后的堆结构应该是(b)。它的计算复杂性分析如下。

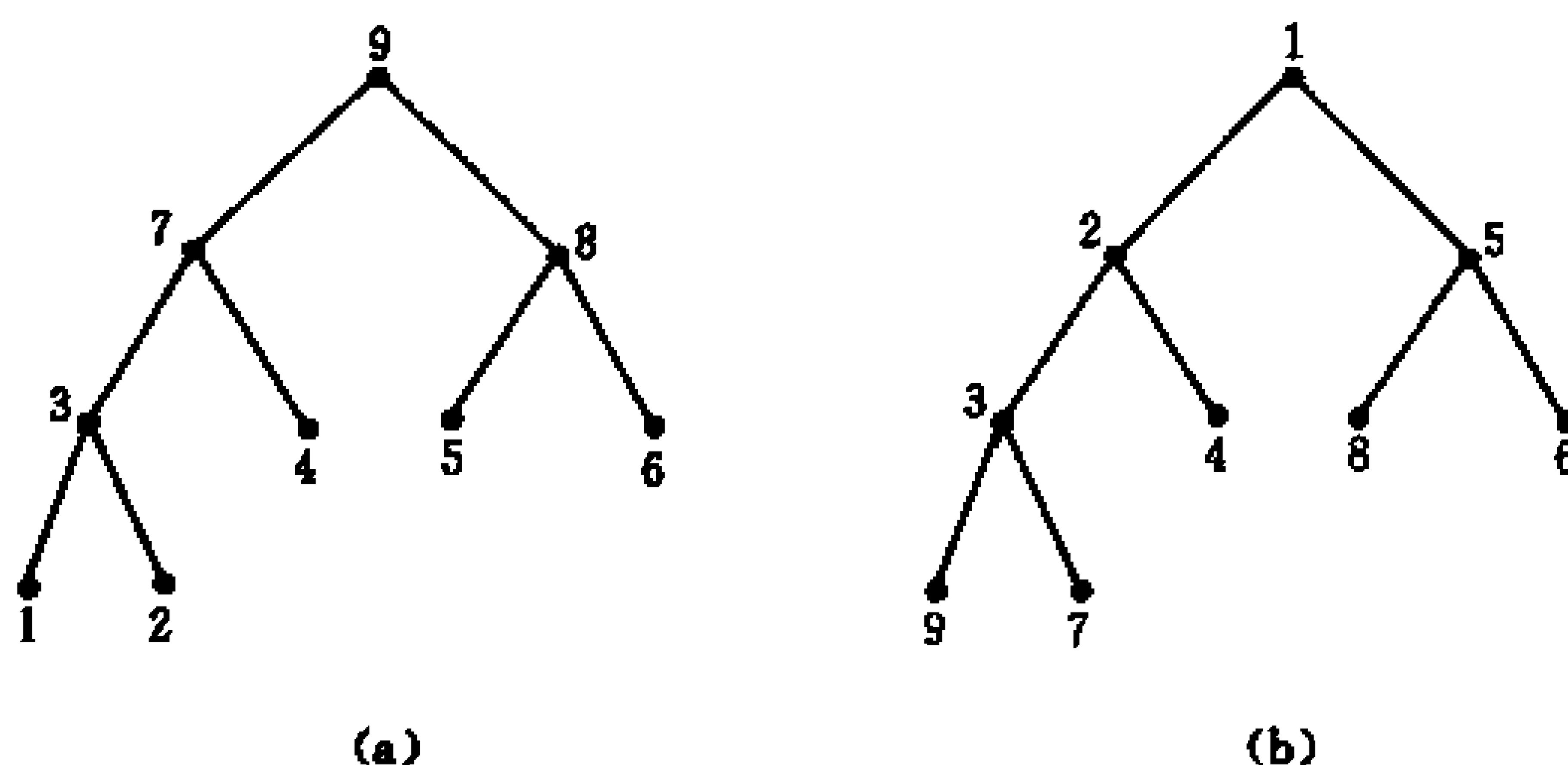


图 3.25

设二叉树的高度即树 T 中根到树叶的最远距离是 h，其结点数目为 N(相当于 G 中的 m 条边)。有

$$N \leqslant 2^0 + 2^1 + \cdots + 2^k + \cdots + 2^h = 2^{h+1} - 1,$$

其中 2^k 表示第 k 层的结点数目。

第 k 层的某结点的权在最坏情况下，会沿着该树的某条路径向下滤到树叶，因此最多有 $2(h-k)$次比较。这样如果第 k 层的全部结点都要向下滤到树叶，就有 $2^k \cdot 2(h-k)$次比较。

所以建堆的总比较次数是

$$S = 2\sum_{k=0}^{h}(h-k)\cdot 2^k = 2h\sum_{k=0}^{h}2^k - 2\sum_{k=0}^{h}k\cdot 2^k = 2h(2^{h+1}-1) - 2S_1,$$

其中

$$S_1 = \sum_{k=0}^{h}k\cdot 2^k = (h-1)2^{h+1} + 2,$$

因此

$$S = 2\cdot 2^{h+1} - 2h - 4 \approx 2N。$$

所以建堆的计算复杂性是 $O(m)$。

当根结点的权(即最短边)取出后，则将最后一个结点删除，把它的权赋予根结点。该二叉树再进行调整，保持其堆结构形式。显然其调整阶段的复杂性是 $\log m$。也就是说每一次迭代时步骤 a 的复杂性是 $\log m$。这样如果算法需要迭代 p 次，步骤 a 的总计算复杂性是 $O(m+p\log m)$。

现在讨论步骤 c。设当前最短边是 $e=(v_i,v_j)$，而先前已选入 T 的边构成的连通支结点集分别是 $V_1,V_2,\cdots,V_t$。当选到 $e=(v_i,v_j)$时，v_i 和 v_j 会处于下列情况之一：

1. v_i,v_j 不属于 $V_1,V_2,\cdots,V_t$ 任一集合。

2. v_i,v_j 之一属于其中某集合 V_k。

3. v_i,v_j 分属于不同的集合 V_k,V_l。

4. v_i,v_j 属于同一集合 V_k。

对情况 1，另设一个结点集 V_q，使 $V_q=\{v_i,v_j\}$；对情况 2，令另一结点 $v_j(v_i)$ 也属于 V_k；对情况 3，令 $V_k \leftarrow V_k \cup V_l$，并删 V_l；对情况 4，因为 v_i,v_j 已属同一连通支，加入此边一定会构成回路，因此 (v_i,v_j) 不能加入 T。这样就可以判别是否构成回路。所以对集合运算来说，算法在步骤 c 的总计算复杂性是 $O(p)$。

这样我们得到

定理 3.7.2 Kruskal 算法的计算复杂性是 $O(m+p\log m)$，其中 p 是迭代次数。

3.7.2 Prim 算法

Prim 算法的基本思想是：首先任选一结点 v_0 构成集合 V'，然后不断在 $V-V'$ 中选一条到 V' 中某点（比如 v）最短的边 (u,v) 进入树 T，并令 $V'=V'+u$，直至 $V'=V$。它的描述如下（设初选 v_1）：

1. $t \leftarrow v_1, T \leftarrow \Phi, U \leftarrow \{t\}$。
2. while $U \neq V$ do

   begin
3. $w(t,u)=\min\limits_{v \in V-U}\{w(t,v)\}$。
4. $T \leftarrow T+e(t,u)$。
5. $U \leftarrow U+u$。
6. for $v \in V-U$ do

   $w(t,v) \leftarrow \min\{w(t,v),w(u,v)\}$。

   end。

显然 Prim 算法的计算复杂性是 $O(n^2)$。

我们仍以图 3.24 为例，说明 prim 算法的执行过程（首选 v_1）。

3. $\min\{w(v_1,v_i)\}=w(v_1,v_2)=15, U=\{v_1\}+v_2$。

6. $w(t,v_3)=w(v_2,v_3)=30, w(t,v_4)=w(v_2,v_4)=20,$

   $w(t,v_5)=w(v_1,v_5)=25$。

3. $\min\{w(t,v_i)\}=w(v_2,v_4)=20, U=\{v_1,v_2\}+v_4$。

6. $w(t,v_3)=w(v_4,v_3)=10, w(t,v_5)=w(v_4,v_5)=10$。

3. $\min\{w(t,v_i)\}=w(v_4,v_3)=10, U=\{v_1,v_2,v_4\}+v_3$。

6. $w(t,v_5)=w(v_4,v_5)=10$。

3. $\min\{w(t,v_i)\}=w(v_4,v_5)=10, U=V$。

结束。

因此最后最短树 $T=\{(v_1,v_2),(v_2,v_4),(v_4,v_3),(v_4,v_5)\}$。

我们再来分析 Prim 算法的正确性。

定理 3.7.3 设 V' 是赋权连通图 $G=(V,E)$ 的结点真子集，e 是二端点分跨在 V' 和 $V-V'$ 的最短边，则 G 中一定存在包含 e 的最短树 T。

证明：设 T_0 是 G 的一棵最短树，若 $e\notin T_0$，则 T_0+e 构成唯一回路。该回路一定包含 e 和 $e'=(u,v)$，其中 $u\in V'$，$v\in V-V'$。由已知条件 $w(e)\leqslant w(e')$，作 $T_0\oplus(e,e')$，得到的仍是最短树。

定理 3.7.4 Prim 算法的结果是得到赋权连通图 G 的一棵最短树。

证明：首先证明它是一棵支撑树。采用归纳法，初始 $U=\{v_1\}$，$T=\Phi$，它是由 U 导出的树，设 $|U|=i$，T 是 U 导出的树，则下一次迭代时，U 中增加一新结点 u，T 中也加入一条与 u 相连的边，因此 T 是连通的，有 $|U|-1$ 条边，它是由 U 导出的一棵树。因此最终 T 是 G 的支撑树。以下再证 T 是一棵最短树。设 T_0 是 G 的一棵最短树，若 $T\neq T_0$，由定理 3.7.3，对任意的 $e\in T-T_0$，一定有最短树 $T'=T_0\oplus(e,e')$，其中 $e'\in C^e\cap T_0$。继续对 T' 如此处理，直至最终 $T'=T$，它仍然是最短树。

Kruskal 算法的复杂性与迭代次数有关，如果图 G 的边数很多，或称是稠密图时，p 值可能较大，也许接近 m。Prim 算法只与 G 的结点有关，而与图的稠密度无关。因此相比较而言，Prim 算法适用于稠密图，而 Kruskal 算法对稀疏图更为合适。

最短树问题一经解决，最长树问题也就迎刃而解。这只要将加入树的边次序按权构成非增序列，采用类似 Kruskal 算法即可实现。有兴趣的读者可以自行设并实现最长树算法。

3.8 最大分枝

上一节讨论了赋权无向图的最短树和最长树，本节将讨论赋权有向连通图 $G=(V,E)$ 的最大权根树等问题。由于有的图并不存在根树，所以也不可能存在最大权根树。比如图 3.26(a)就没有根树。但是对任何有向图都存在仅由外向树组成的支撑子图，这种支撑子图就叫做 G 的分枝。比如图 3.26(b)就是(a)的一个分枝。显然任何赋权有向图都存在最大权分枝，即分枝中边权的和为最大。

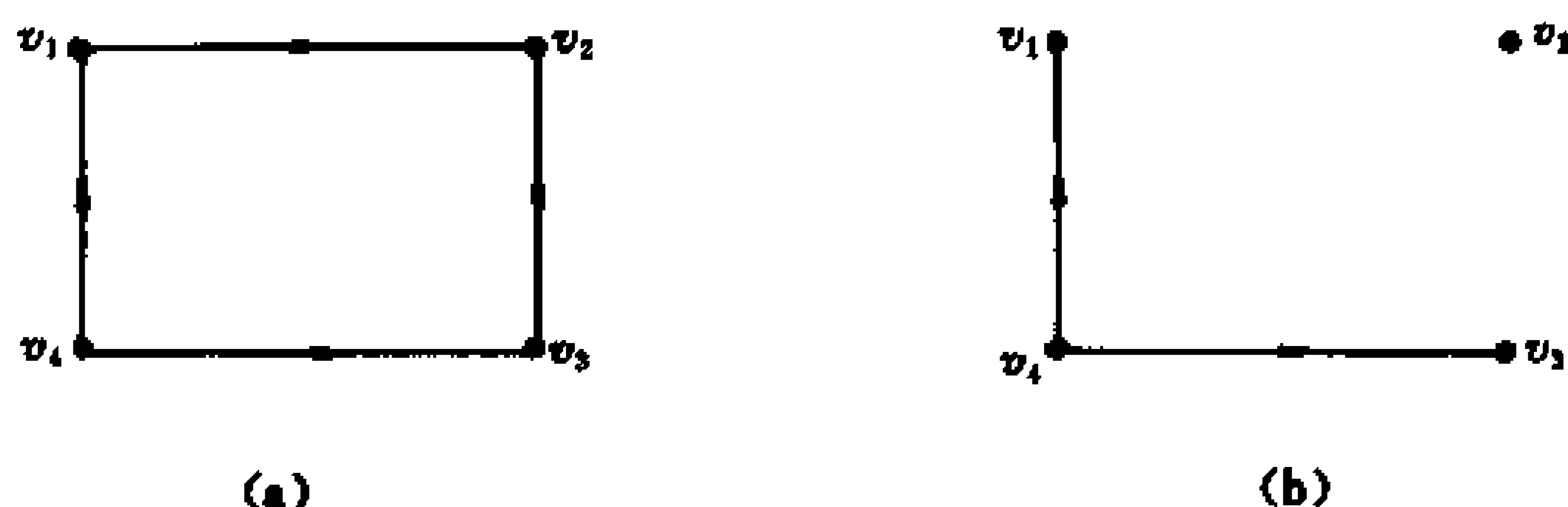


图 3.26

如果我们能够构造和计算赋权有向图 G 的最大分枝，那么稍加改变，就可以计算一个图 G 的最小分枝，最大(小)权根树，以及根在规定结点的最大(小)权根树(如果存在)，比如：

1. 最小分枝。取一大数 M，$M\geqslant\max_{e\in E}w(e)$。对 G 中的每条边 e，改变其权值为 $w'(e)=M-w(e)$。得到图 G'。则 G' 的最大分枝对应于 G 的最小分枝。

2. 最大权根树(如果存在)。应该指出，G 中如果有最大权根树，它也不一定就是 G 的

最大分枝。例如图 3.27 的最大权根树是$\{(v_1,v_2),(v_2,v_3)\}$，而最大分枝是$\{(v_3,v_2)\}$。但是如果对 G 的每条边权都加上一个足够大正数 M，则其最大分枝就对应 G 的一个最大权根树。比如图 3.27 每边的权都增加 10，其最大分枝亦将是$\{(v_1,v_2),(v_2,v_3)\}$。

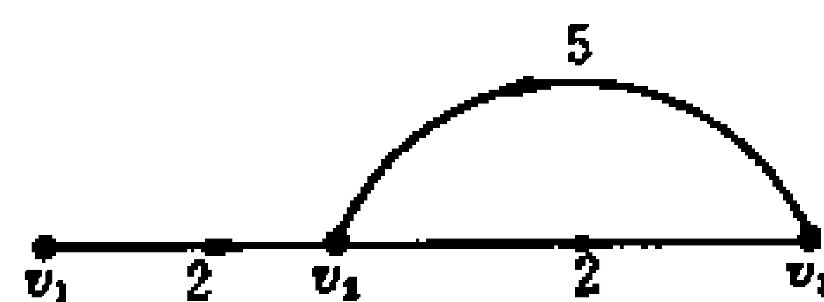


图 3.27

3. 以规定结点 v_0 为根的最大权根树(如果存在)，对 G 增加一个结点 s，增加一条有向边(s,v_0)，令 $w(s,v_0)=\sum_{e\in E(G)} w(e)$。这样得到一个新的赋权图 G'。显然 G' 也一定存在最大权根树，而且根在 s，因为它的负度为 0。舍去边(s,v_0)，就得到 G 的以 v_0 为根的最大权根树。

现在我们来介绍 Edmonds 提出的最大分枝算法。

最大分枝问题要求：a)不能产生回路；b)每个结点的负度最多为 1；c)在满足条件 a、b 的基础上，使得分枝中的边权总和为最大。这样，最初令最大分枝的结点集 BV 和边集 BE 都为空。然后对任意结点 $v\in V-BV$，选其具有最大权的入边 $e=(u,v)$，令 $BV\leftarrow BV+v$，$BE\leftarrow BE+e$。如果此时没有构成回路(只能是有向回路)，这时 BE 仍是 G 的分枝。如果构成了回路 C_1，则把 C_1 中的各结点收缩成一个新的结点 u_1，G 变成一个含有结点 u_1 的新图 G_1，G_1 仍保持 G 内原有的邻接关系。比如图 3.28(a)的回路 $C=(v_1,v_2,v_3)$收缩成 u_1 后，得到的 G_1 如(b)所示。在 G_1 中所有进入 u_1 的边权要进行适当调整，这样 G_1 中的分枝不存在回路，对 G_1 继续上述过程，最后得到 G_i 的一个分枝

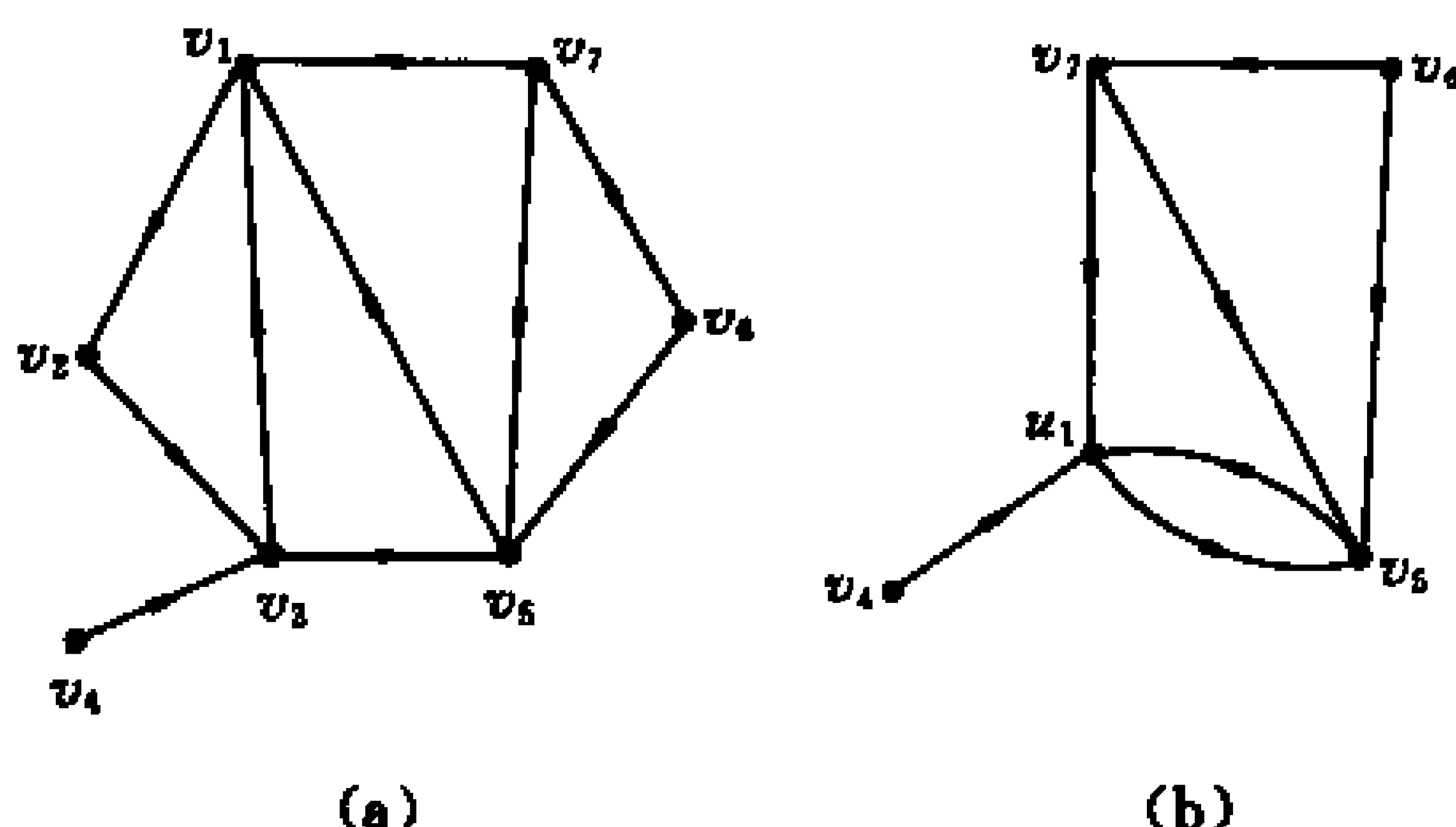


图 3.28

很明显，最终 G_i 里包含了 i 个结点 u_j。每个 u_j 对应于原图 G 的某个独立回路。因此 G_i 的分枝不可能是 G 的分枝，不过当从 G_i 退回到 G_{i-1}时，首先要将结点 u_i 还原成回路 C_i。这时只有舍弃 C_i 中的一条边后，其余边加上原来 G_i 分枝的边才能构成 G_{i-1}的一个分枝。为了得到最大分枝，当然应该舍弃 C_i 中影响最小的边。将这种还原过程重复下去，直至恢复到 G 为止，这时 BE 中的各边就构成了 G 的最大分枝。设最初的图是 $G_0=(V_0,E_0)$，$G_i=(V_i,E_i)$是 u_i 代替回路 C_i 得到的图。

最大分枝的 Edmonds 算法描述如下：

1. BV←Φ，BE←Φ。

2. i←0。

3. 若 BV=V_i，转 14。

4. 对某个结点 $v \in V_i - BV$，

begin

5. $BV \leftarrow BV + v$。

6. 找一条边 $e=(x,v)$，满足

$$w(e)=\max\{w(y,v)\mid(y,v)\in E_i\}。$$

7. 若 $w(e)\leqslant 0$，转 3。

end

8. 若 $BE+e$ 构成回路 C_i，

begin

9. $i \leftarrow i+1$。

10. 将 C_i 收缩成结点 u_i，构成 G_i。

11. 修改 BE，BV 和某些边权。

end

12. $BE \leftarrow BE+e$。

13. 转 3。

14. while $i \neq 0$ do

begin

15. 重构 G_{i-1} 及 BE 中的某些边。

16. 若 u_i 是 BE 中一个外向树的根，则

17. $BE \leftarrow BE \cup \{e \mid e \in C_i, e \neq e_i^0\}$，

18. 否则 $BE \leftarrow BE \cup \{e \mid e \in C_i, e \neq \tilde{e}_i\}$。

19. $i \leftarrow i-1$。

end

20. 最大分枝权为 $\sum\limits_{e \in BE}^{H} w(e)$。

在算法的第 10 行，G_i 的结点包括 G_{i-1} 中所有不在 C_i 上的结点以及 u_i，E_i 包括(1) E_{i-1} 中全部不与 C_i 的某结点相关联的边，其权不变；(2)如果 $e=(x,y)\in E_{i-1}$，$x\in C_i$，$y\notin C_i$，则 $e'=(u_i,y)\in E_i$，权不变；(3)若 $e=(x,y)$，$x\notin C_i$，$y\in C_i$，则 $(x,u_i)\in E_i$，$w(x,u_i)=w(e)-w(\tilde{e})+w(e_i^0)$。其中 $\tilde{e}$ 是 C_i 中进入结点 y 的边，e_i^0 是 C_i 中权最小的边。例如图 3.29(a)中，当回路 $C=(v_1,v_2,v_3)$ 收缩成 u_i 之后，对 $e=(v_5,v_1)$，$e_i^0=(v_1,v_2)$，$\tilde{e}=(v_3,v_1)$，于是 $w(v_5,u_i)=1-4+2=-1$。同理，$w(v_4,u_i)=0$，$w(v_6,u_i)=1$。如图 3.29(b)。

在执行 14～19 行的 while 语句时，回路 $C_i, C_{i-1}, \cdots, C_1$ 将依次包含在分枝中。在第 15 行从 G_i 重构 G_{i-1} 时，可能有两种情况：

a. 结点 u_i 是 E_i 分枝中某个子树的根。

b. 结点 u_i 不是 E_i 分枝中某个子树的根。

如果出现 a 这种情况，则 BE_{i-1} 中恰含一个回路 C_i，舍弃 C_i 中权最小的边，显然会得到 G_{i-1} 的一个最大分枝。如果情况 b 出现，则 BE_i 中有唯一一条指向 u_i 的边 (x,u_i)，(x,u_i) 对应 G_{i-1} 的一条边 (x,y)。结点 y 在 G_{i-1} 中的 BE_{i-1} 里已有两条进入边：(x,y) 和 $\tilde{e}$。因此

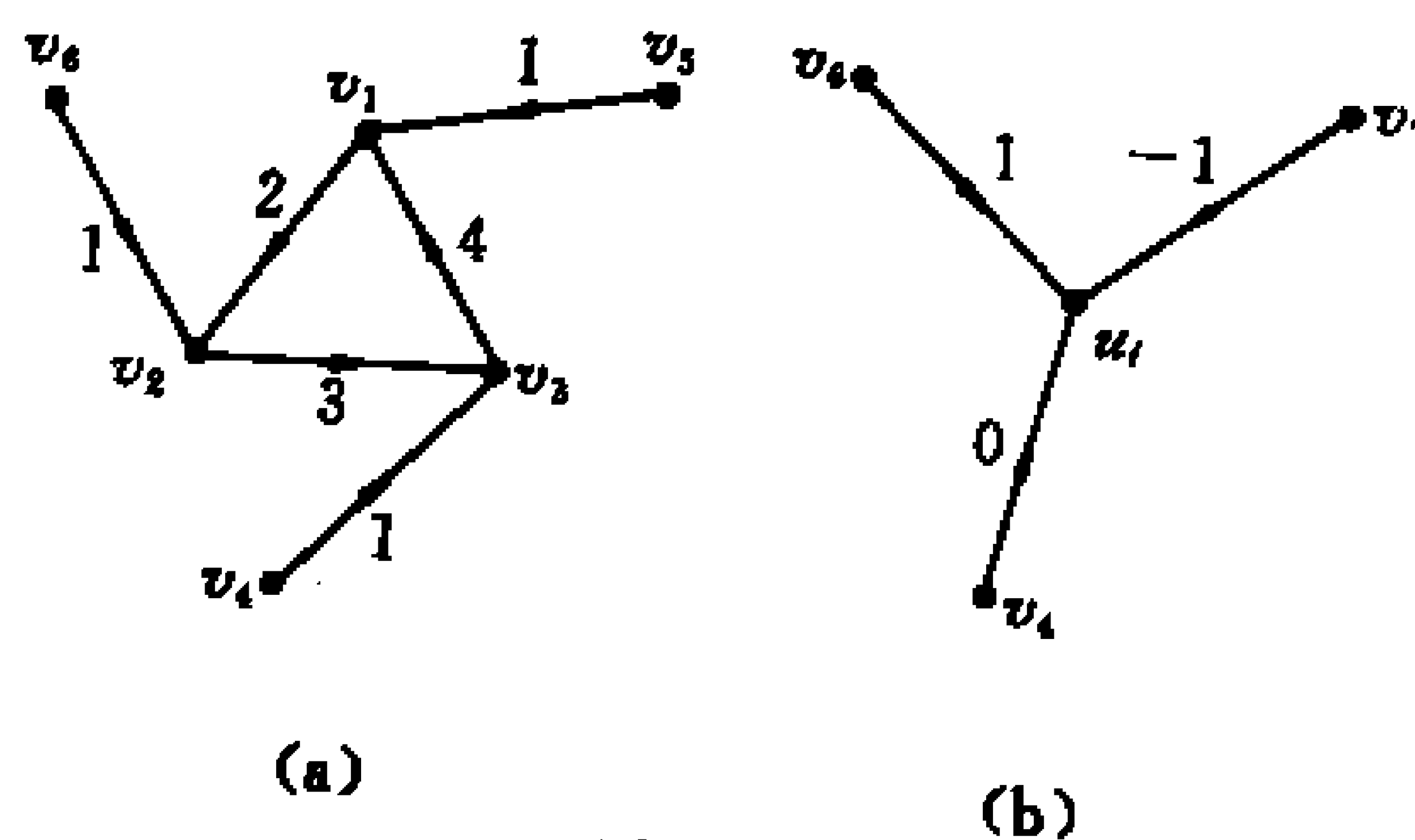


图 3.29

只有舍弃 $\bar{e}$，才能使 BE_{i-1}构成 G_{i-1}的一个分枝。

例 3.8.1 用 Edmonds 算法计算图 3.30 的最大分枝的过程如下：

(a)构造 $G_1,G_2,\cdots,G_k$。

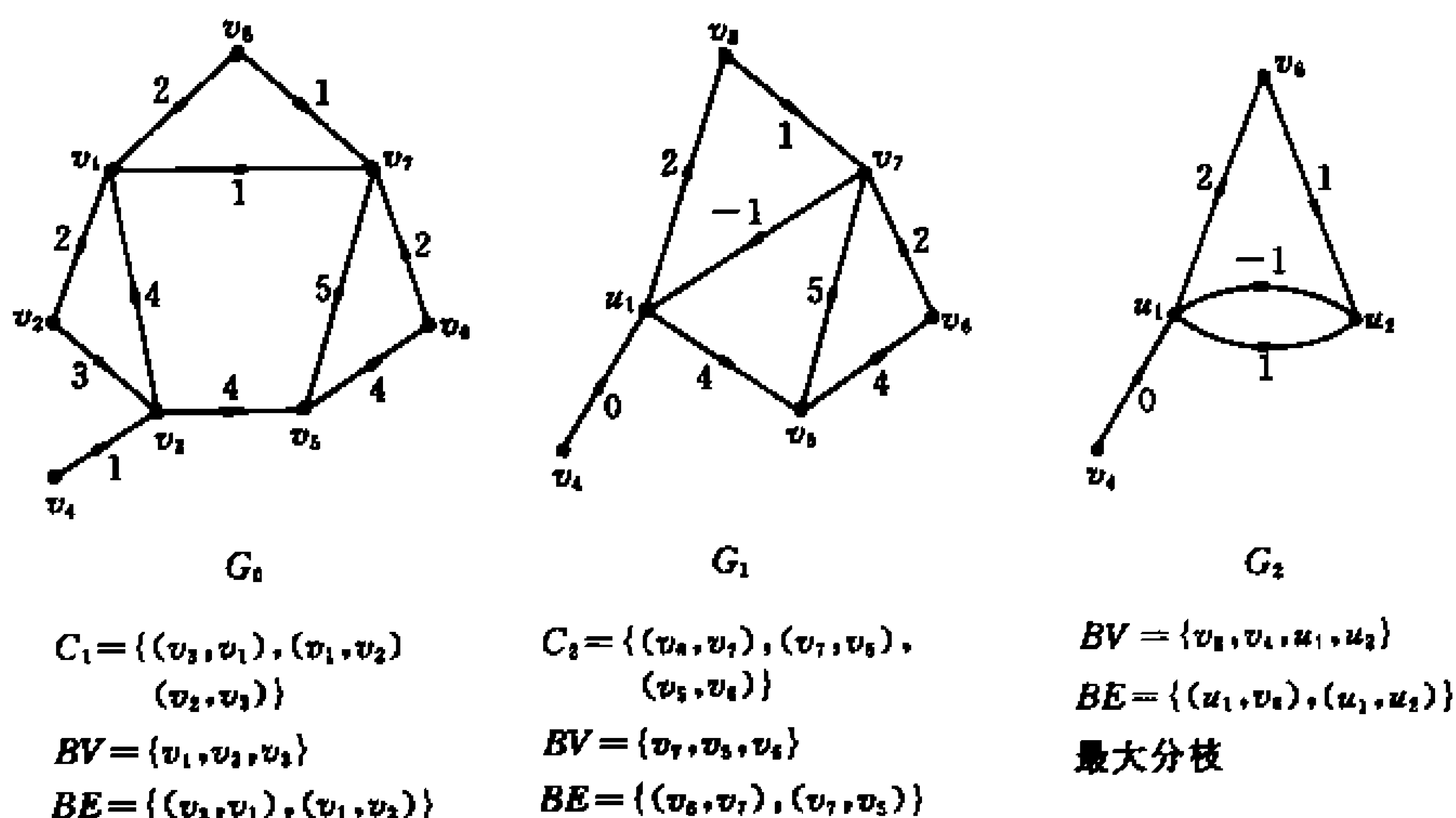


图 3.30

(b)重构 $G_{k-1},G_{k-2},\cdots,G_0$。

G_2：$BE=\{(u_1,v_8),(u_1,u_2)\}$。

G_1：$BE=\{(u_1,v_8),(u_1,v_5),(v_5,v_6),(v_6,v_7)\}$。

G_0：$BE=\{(v_1,v_8),(v_3,v_5),(v_2,v_3),(v_3,v_1),(v_5,v_6),(v_6,v_7)\}$。

其最大分枝权是 19。

定理 3.8.1 Edmonds 算法的结果是 G 的一个最大权分枝。

证明：我们将证明。如果 BE 包含了最终构造的图 G_k 的最大分枝，在结点展开后，BE 中的边恰好构成了 G_0 的一个最大分枝。

初始，当第 3 行检测 BV 包含了 V_k 的全部结点时，对 V_k 的每个结点，都最多有一条最大权的进入边属于 BE，而且它们构成了 G_k 的一个分枝，即是最大分枝。

假设，BE_i 包含了 G_i 最大分枝各边，考虑 G_{i-1}和相应的边集 BE_{i-1}。由算法过程知道，G_i 是由于 G_{i-1}中出现了回路 C_i 形成新结点 u_i 而得到的，因此当退回到 G_{i-1}时，只能出现下述情况之一：

1. 分枝 BE_i 不包含形如(x,u_i)的边。即 C_i 中有一个结点将是 G_{i-1}中某个子树的根。由于 C_i 的每个结点在 G_{i-1}中都有一条最大权入边，而 BE_{i-1}不可能全部包含它们，而必须舍弃其一。由于 e_i^0 是其中的最短边，所以

$$BE_i \cup \{e \mid e \in C_i,\ e \neq e_i^0\}$$

包含了 G_{i-1}最大分枝诸边，这由算法的 17 行实现。

2. 分枝 BE_i 包含了一条(x,u_i)边，此时，已经有

$$w(x,u_i) = \max(w(x,y) - w(\tilde{e}_i) + w(e_i^0)) > 0，其中\ y \in C_i$$

由于对任何满足

$$w(e) - w(\tilde{e}_i) + w(e_i^0) > 0$$

的边 $e=(x,y)$，都有

$$w(C_i) + w(e) - w(\tilde{e}_i) > w(C_i) - w(e_i^0)$$

因此，保留 C_i 中的最短边 e_i^0，删去 $\tilde{e}_i$ 能得到更大的权值。而(x,u_i)是选用了进入 u_i 的最大权边，所以在返回 G_{i-1}时，BE_{i-1}包含了它的最大分枝。它由算法第 18 行实现。

综上，BE_{i-1}中各边构成了 G_{i-1}的最大分枝。证毕。

定理 3.8.2 Edmonds 算法的计算复杂性是 $O(mn)$。

证明：算法占用时间最多的是图的收缩和扩充，即第 10 行和 15 行。在每次收缩（或扩充）时，需要检查每条边，因此其计算复杂性是 $O(m)$，而收缩（或扩充）不可能多于 n 次。此外，第 6 行和第 8 行也较为复杂，对每个结点 v_i，找其最大权入边需要 $d^-(v_i)-1$ 次比较，因此第 6 行的总比较次数是 $O(m)$，而第 8 行检测一个回路的复杂性是 $O(n)$。因此整个算法的计算复杂性是 $O(mn)$。

习 题 三

1. 一棵树有 n_2 个结点的度为 2，n_3 个结点的度为 3，…，n_k 个结点的度为 k。问有多少个度为 1 的结点。

2. 证明树中最长道路的两端点一定都是树叶。

3. 令 $v_1,v_2,\cdots,v_n$ 是给定结点，$d_1,d_2,\cdots,d_n$ 是给定的数，满足 $\sum d_i = 2n-2, d_i \geqslant 1$。证明在集合 $V=\{v_1,v_2,\cdots,v_n\}$上满足 $d(v_i)=d_i, i=1,2,\cdots,n$ 的树的数目是

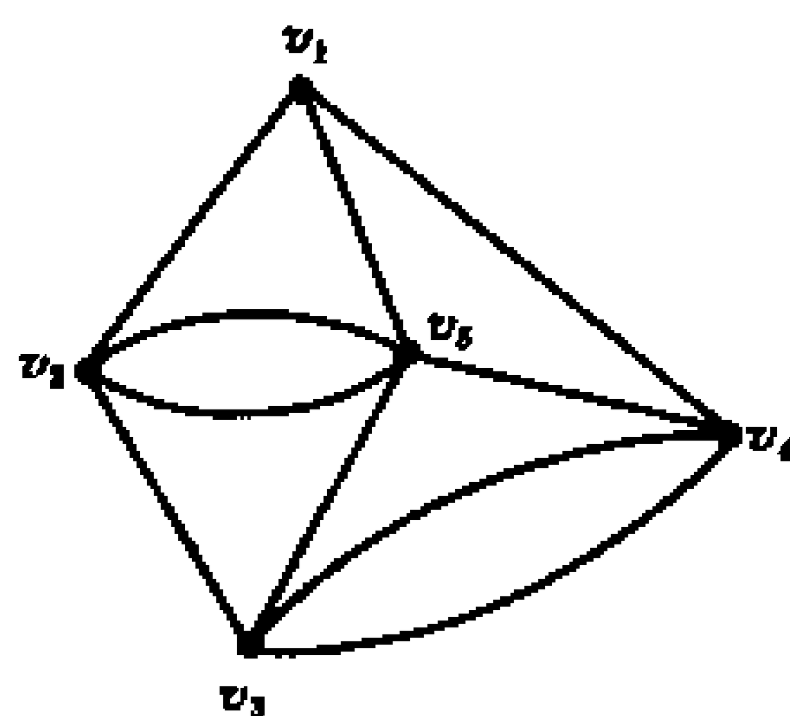
$$\frac{(n-2)!}{(d_1-1)!\cdots(d_n-1)!}。$$

4. 求图中

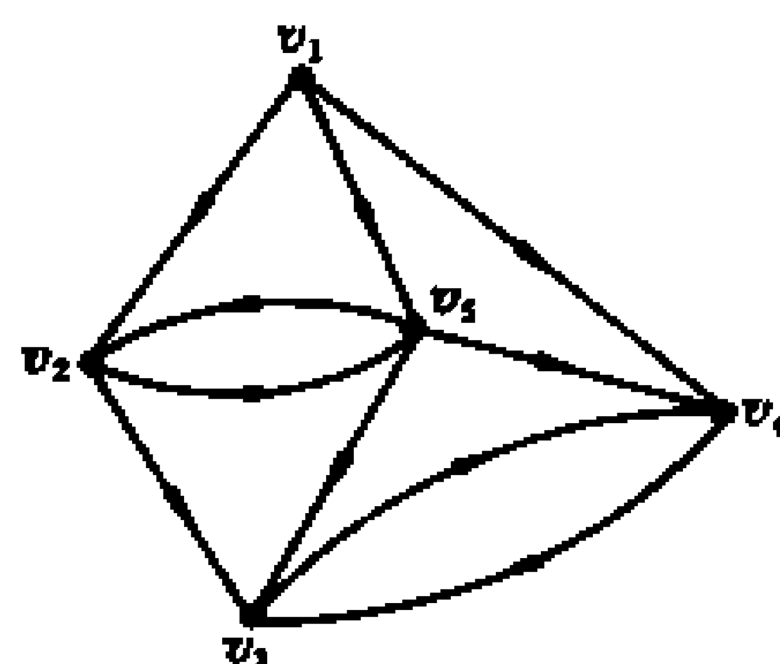
(a)树的数目。

(b)必含(v_1,v_5)的树的数目。

(c)不含(v_4,v_5)的树的数目。



题图 3.4



题图 3.5

5. 求图中

(a)以 v_1 为根的根树数目。

(b)以 v_1 为根不含(v_1,v_5)的根树数目。

(c)以 v_1 为根必含(v_2,v_3)的根树数目。

6. 求 K_n 中不含某特定边(v_i,v_j)的树的数目。

7. 求 K_n 中必含某特定边(v_i,v_j)的树的数目。

8. 证明完全二分图 $K_{m,n}$的树的数目是 $m^{n-1}n^{m-1}$。

9. 举例说明,$\det(\overrightarrow{B}_k\overrightarrow{B}_k^T)$ 不是以 v_k 为根的根树数目。

10. 已知连通图 G 的基本关联矩阵是

$$B_5=\begin{bmatrix}-1 & 1 & 0 & 0 & 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0\\ 0 & -1 & -1 & 0 & 0 & 0 & -1 & 0\\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & -1\end{bmatrix}$$

$$\quad e_1 \quad e_2 \quad e_3 \quad e_4 \quad e_5 \quad e_6 \quad e_7 \quad e_8$$

求(1)以$\{e_3,e_4,e_6,e_7\}$为树的基本回路矩阵。

(2)以$\{e_2,e_5,e_6,e_8\}$为树的基本割集矩阵。

11. 已知矩阵C'包含了连通图 G 的回路矩阵,求 G 的以$\{e_5,e_6,e_7,e_8\}$为树的基本割集矩阵。

$$C'=\begin{bmatrix}1 & 0 & 0 & 0 & -1 & -1 & 0 & 0\\ 1 & 0 & 1 & 0 & -1 & 0 & -1 & 0\\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1\\ -1 & -1 & 0 & 1 & 0 & 0 & 0 & 0\end{bmatrix}$$

$$\quad e_1 \quad e_2 \quad e_3 \quad e_4 \quad e_5 \quad e_6 \quad e_7 \quad e_8$$

12. 设完全 m 叉树中,树叶数为 t,分枝结点数是 i,证明:$(m-1)i=t-1$。

13. 设 G 是无向图,对任意结点 $v\in V(G)$,$G-v$ 仍是连通图,而且 G 的基本割集矩阵 S_f 的每一行都有偶数个 1 元素。证明 G 中有欧拉回路。

14. 给出字符串 state act as a seat

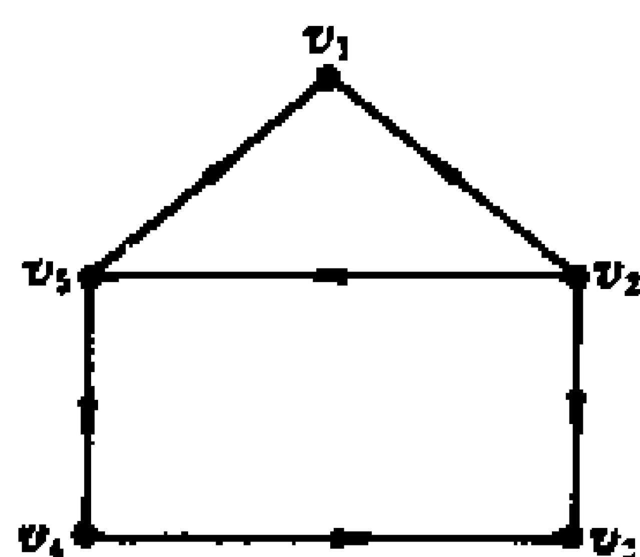
(a)最优二进制编码。

(b)如果二进制字符串不允许带空格，求该字符串的最优二进制编码。

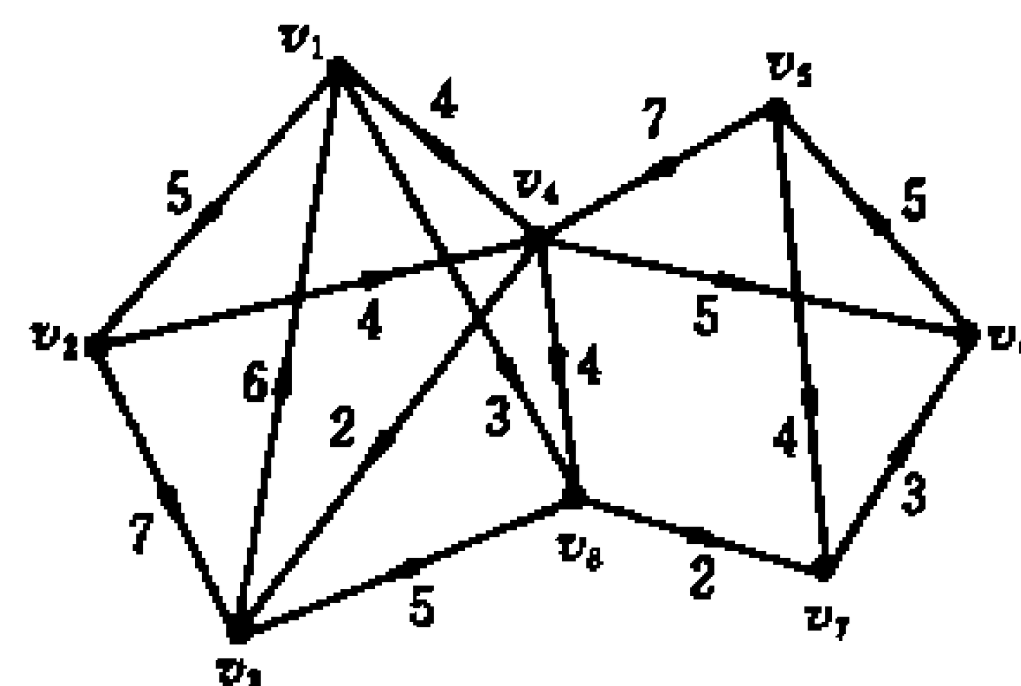
15. 用 Mayeda 算法求图的全部生成树。

16. 求图的最短树。

17. 求图的最大分枝。



题图 3.15



题图 3.16、3.17

18. 编写实现 Huffman 算法的程序。

19. 编写实现 Mayeda 算法的程序。

20. 编写求最短树的程序。

21. 编写求最大分枝的程序。

第四章　平面图与图的着色

4.1 平 面 图

在实际问题中有时要涉及到图的平面性的讨论，比如印刷电路板的设计、大规模集成电路的布局布线等，都离不开图的平面性研究。著名的四色猜想也属于平面性范畴。

定义 4.1.1　若能把图 G 画在一个平面上，使任何两条边都不相交，就称 G 可嵌入平面，或称 G 是可平面图。可平面图在平面上的一个嵌入称为平面图。

例如图 4.1(b)、(c)都是(a)的一个平面嵌入，因此(a)是可平面图，(b)、(c)都是(a)的一个平面嵌入，是平面图。

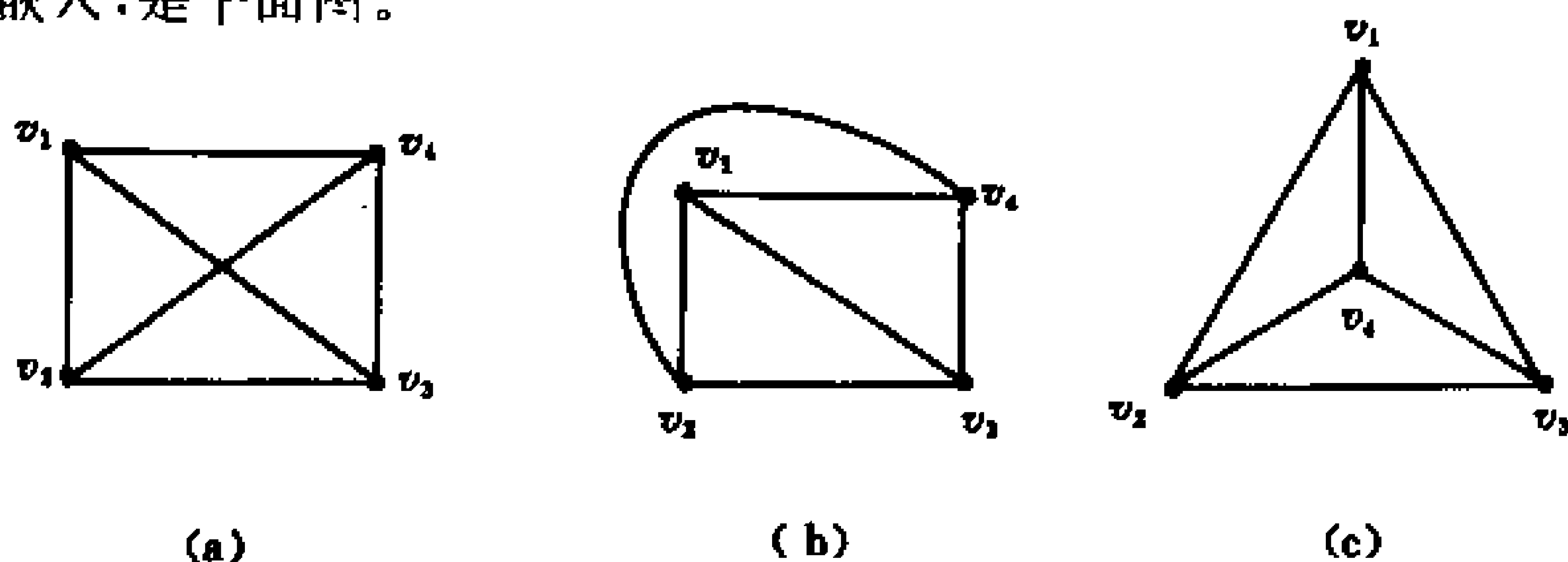


图 4.1

显然，如果 G 是可平面图，那么它的任何导出子图也是可平面图。

定义 4.1.2　设 G 是一个平面图，由它的若干条边所构成的一个区域内如果不含任何结点及边，就称该区域为 G 的一个面或域。包围这个域的诸边称为该域的边界。

为了讨论方便，我们把平面图 G 外边的无限区域称为无限域，其它的域都叫内部域。如果两个域有共同的边界，就说它们是相邻的，否则是不相邻的。如果 e 不是割边，它一定是某两个域的共同边界。

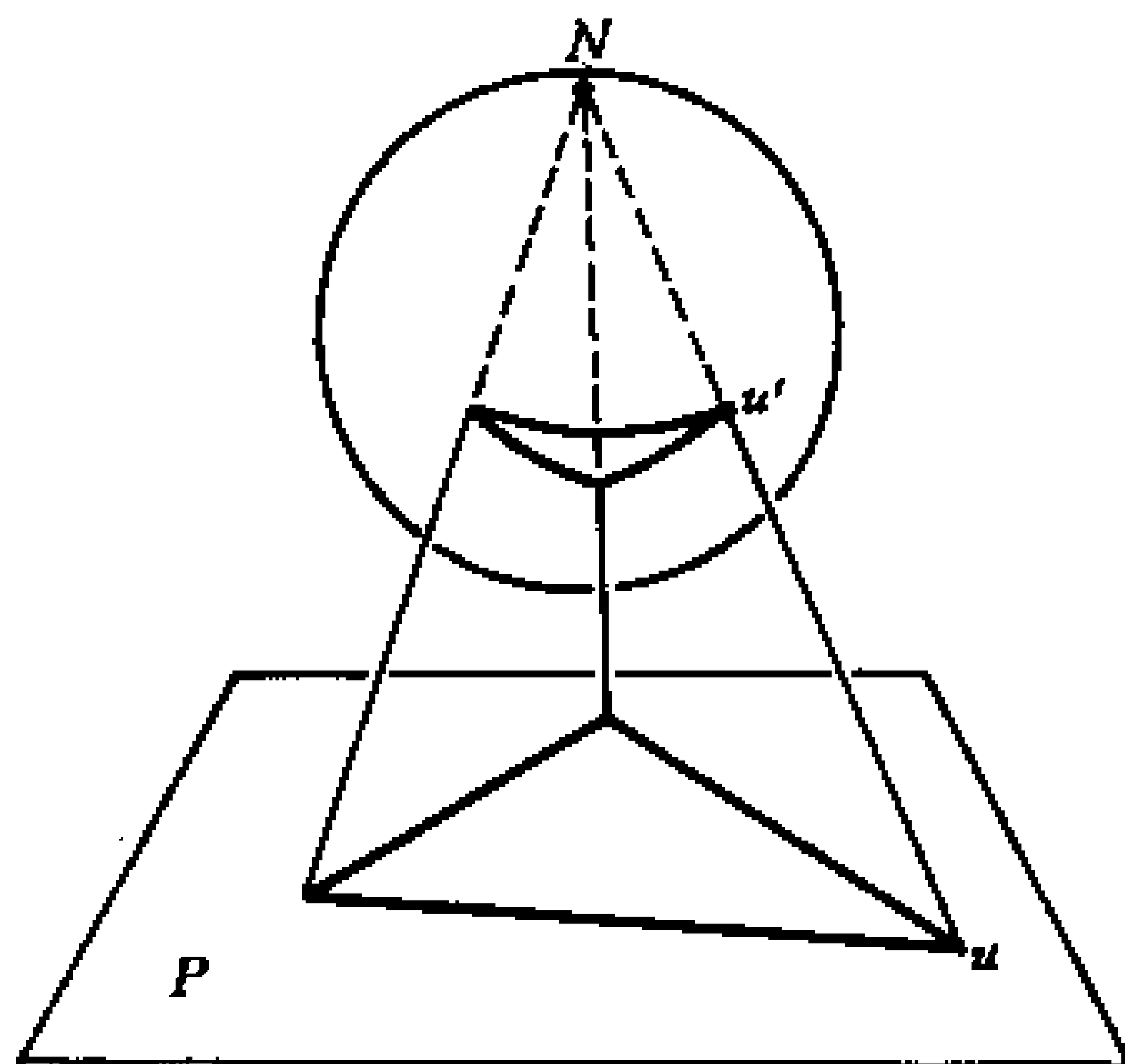


图 4.2

事实上，平面图早已为大家所熟悉，世界地图就是一个平面图。这也就是说，一个图 G 是可平面的等价于它是可球面的。这一论断可以通过“测地变换”来实现。设 N 是球面的北极，平面 P 在球的下方，则平面上的任一点 u 与 N 的连线必过球面上的唯一点 u'。即球面上的点与平面上的点存在一一对应，因此平面上的一个域对应球面上的一个域，其中无限域对应 N 所在的内部域。

这样通过测地变换可以把平面图 G 的任何一个内部域改换为无限域：先用测地变换

把 G 画到球面上，然后把 N 设置在预定的域 d_i 中，再通过测地变换把图画到平面上，这时 d_i 就变成了无限域。例如图 4.1(b)和(c)的无限域是不一样的，它在(b)中的边界是 (v_2,v_3)，(v_3,v_4)和 (v_4,v_2)，在(c)里的边界是(v_1,v_2)，(v_2,v_3)，(v_3,v_1)。

下面介绍平面图的一个最基本的定理——欧拉公式。

定理 4.1.1 设 G 是平面连通图，则 G 的域的数目是

$$d = m - n + 2。$$

证明：G 是连通图，有支撑树 T，它包含 $n-1$ 条边，不产生回路，因此对 T 来说只有一个无限域。由于 G 是平面图，每加入一条余树边，它一定不与其它边相交，也就是说一定是跨在某个域的内部，把该域分成两部分。这样，加入 G 的 $m-n+1$ 条余树边，就生成了 $m-n+2$ 个域。

推论 4.1.1 若平面图 G 有 k 个连通支，则

$$n - m + d = k + 1。$$

推论 4.1.2 对一般平面图 G，恒有

$$n - m + d \geqslant 2。$$

定理 4.1.2 设平面连通图 G 没有割边，且每个域的边界数至少是 t，则

$$m \leqslant \frac{t(n-2)}{t-2}。$$

证明：设 G 有 d 个域，每个域的边界数至少是 t，且每条边都与两个不同的域相邻。因此 $td \leqslant 2m$。代入欧拉公式。

$$\frac{2m}{t} \geqslant m - n + 2,$$

亦即

$$m \leqslant \frac{t(n-2)}{t-2}。$$

4.2 极大平面图

本节只限于讨论简单平面图。

定义 4.2.1 设 G 是 $n \geqslant 3$ 的简单平面图，若在任意两个不相邻的结点 v_i, v_j 之间加入边 (v_i, v_j)，就会破坏图的平面性，就称 G 是极大平面图。

有时给定 G 之后，加入某条边 $e=(v_i,v_j)$ 总会与其它边相交，但 $G+e$ 可能仍然是可平面的。这时不能说 G 是极大平面图。比如往图 4.3(a)中加入(v_3,v_5)总要与其余某些边相交。而当改画一下边(v_2,v_4)后，再加入(v_3,v_5)并没有破坏其平面性，如图 4.3(b)所示，因此说(a)并不是极大平面图。

极大平面图 G 具有以下性质：

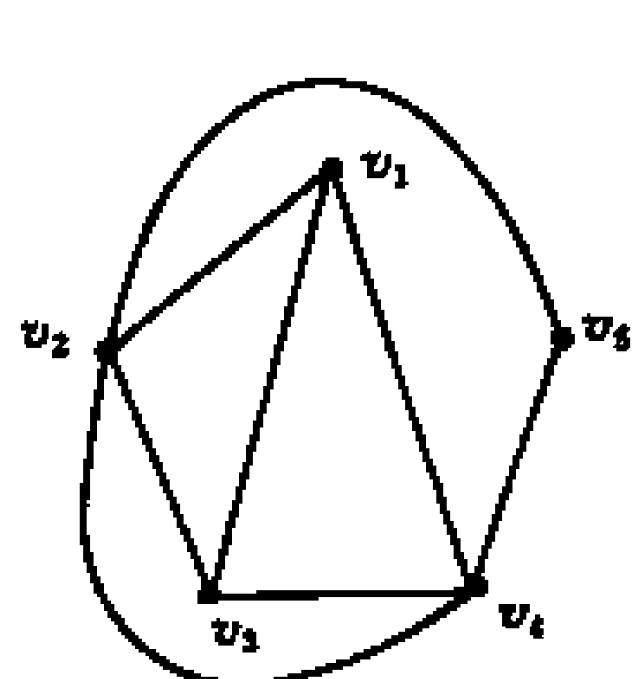
性质 1. G 是连通的。

性质 2. G 不存在割边。

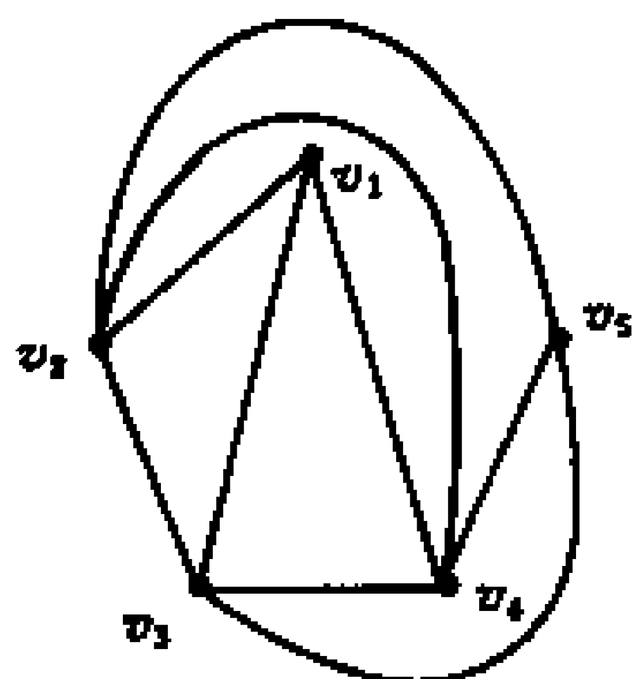
性质 3. G 的每个域的边界数都是 3。

其中性质 3 的证明如下：因为 G 是简单图，没有自环和重边，因此不存在边界数为 1

和 2 的域。假定 G 存在边界数大于 3 的域 d_j，不妨设 d_j 是其内部域，如图 4.4 所示。若结点 i_1 和 i_3 不相邻，则在域 d_j 内加入 (i_1,i_3) 仍是平面图，与 G 是极大平面图矛盾，因此边 (i_1,i_3) 一定存在于域 d_j 之外。而这时，在 d_j 之外不可能存在边 (i_2,i_4)。亦即 i_2,i_4 不相邻，但在域 d_j 内加入边 (i_2,i_4) 并不影响 G 的平面性。矛盾。



(a)



(b)

图 4.3

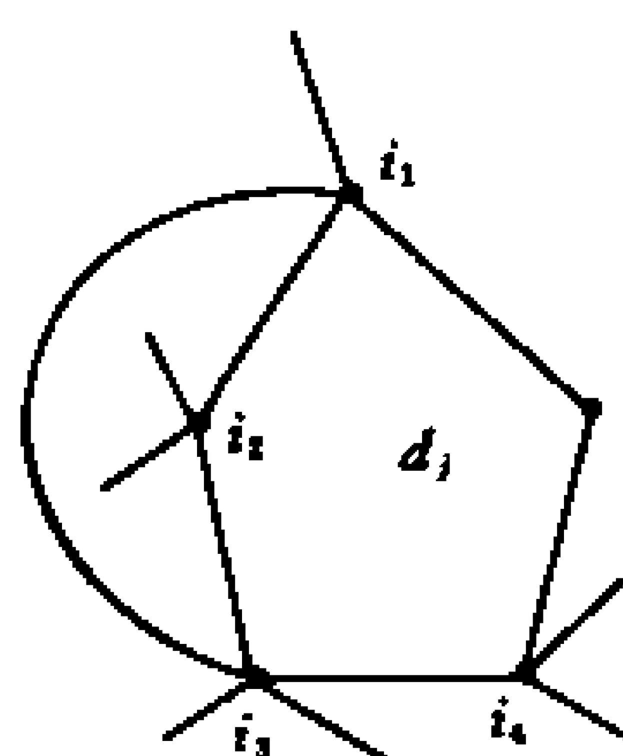


图 4.4

性质 4.　$3d=2m$。

由性质 2，每条边都是两个不同域的边界，再由性质 3 即得。

定理 4.2.1　极大平面图 G 中，有

$$m=3n-6,\qquad d=2n-4。$$

证明：由极大平面图的性质 4

$$3d=2m$$

代入欧拉公式

$$d=m-n+2,$$

整理后即得。

推论 4.2.1　简单平面图 G 满足

$$m\leqslant 3n-6,\quad d\leqslant 2n-4。$$

证明：设 G 中没有割边，因为 G 中没有自环和重边，所以每个域的边界数至少为 3，故 $3d\leqslant 2m$。如果 G 里有割边 e，由于 e 并不能增加 G 的域数，也有 $3d<2m$。代入欧拉公式即得。

例 4.2.1　若简单平面图 G 有 6 个结点 12 条边，则每个域的边界数都是 3。

证明：由 $n=6,m=12$，满足定理 4.2.1 的 $m=3n-6$，因此 G 是极大平面图，每个域的边界数都是 3。

例 4.2.2　若简单平面图 G 不含 K_3 子图，则有

$$m\leqslant 2n-4。$$

证明：显见每个域的边界数至少为 4，因此可得 $4d\leqslant 2m$，代入欧拉公式，

$$\frac{m}{2}\geqslant m-n+2,$$

即

$$m\leqslant 2n-4。$$

定理 4.2.2　简单平面图 G 中存在度小于 6 的结点。

证明：设每个结点的度都不小于 6，由$\sum d(v_i)=2m$，得到 $6n\leqslant 2m$。因为 G 是简单平面图，又有 $3d\leqslant 2m$。代入欧拉公式的一般形式

$$n-m+d\geqslant 2,$$

有

$$\frac{1}{3}m-m+\frac{2}{3}m\geqslant 2,$$

矛盾。

例 4.2.3 结点数不超过 11 的简单平面图 G 一定存在度小于 5 的结点。

证明：假定每结点的度都不小于 5，则 $5n\leqslant 2m$，由 G 是平面图，满足 $m\leqslant 3n-6$，因此得 $n\geqslant 12$。与已知条件矛盾。

例 4.2.4 K_7 图不是平面图。

证：因为 K_7 图每个结点的度均为 6。由定理 4.2.2 即得证。

4.3 非平面图

如果图 G 不能嵌入平面，满足任意两边只能在结点处相交，那么 G 就称为非平面图。比如在某个极大平面图的任意不相邻两点间再添加一条边，就是非平面图；有的平面图 G 虽然不是极大平面图，但是添加某条确定的边 e 时，$G+e$ 就不能嵌入平面，它也是非平面图。这样，按平面性进行划分，图 G 分为两大类：可平面图和非平面图。那么是否存在区分它们的准则呢？我们先考察最简单的非平面图。亦即，在结点数最少的前提下再让边数最少的那些非平面图。

如果图 G 不是简单图，可以首先删去自环和重边，因为它们不影响图的平面性。因此只考虑简单图。我们知道 K_3，K_4 是可平面的，如图 4.1。从图 4.3 也可知道，给定一条边 e，K_5-e 是可平面的。

定理 4.3.1 K_5 是非平面图。

证明：在 K_5 中，$n=5$，$m=10$。如果它是可平面图，应有 $m\leqslant 3n-6$。而此时 $3n-6=9$，矛盾。

这样我们得到了一个结点数最少的非平面图，如图 4.5。当结点数为 6 时，边数最少的非平面图又将是怎样的呢？

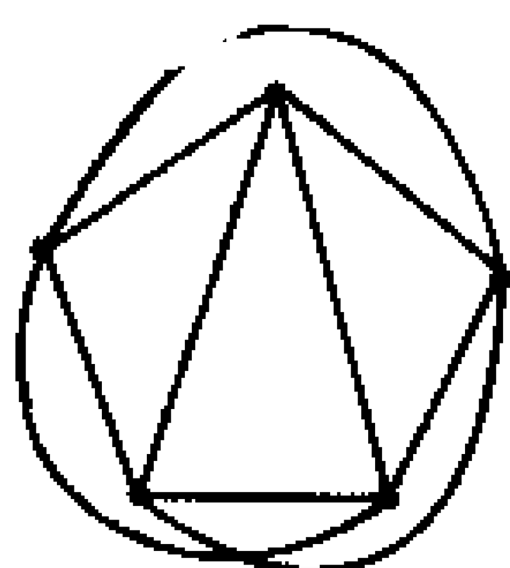
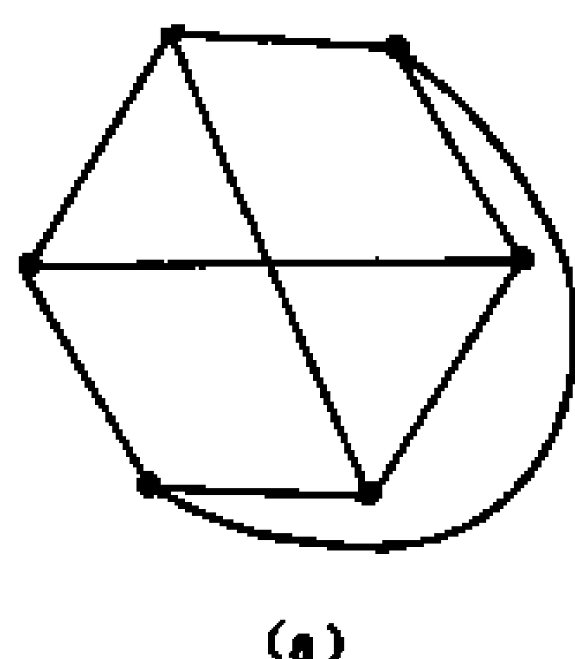
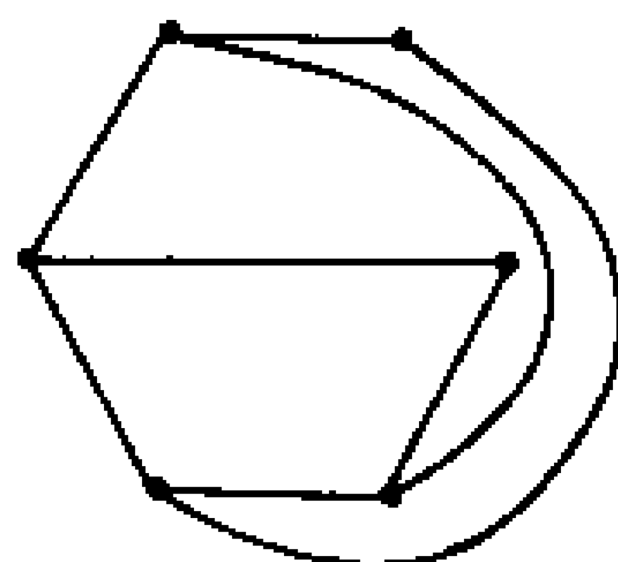


图 4.5



(a)



(b)

图 4.6

例 4.3.1 在图 4.6(a)中,如果任意去掉一条边,G 将是可平面图。显然任意移去一条对角边,G 将是可平面;任意移去另外一条边,比如 e,也将是可平面的,(b)就是它的一个平面嵌入。图 4.6(a)事实上就是二分图 $K_{3,3}$。

定理 4.3.2 $K_{3,3}$是非平面图。

证明:假定 $K_{3,3}$是可平面图,由于 $n=6,m=9$。由欧拉公式,$d=5$。但 G 中没有 K_3 子图,因此 $4d\leqslant 2m$,亦即 $20\leqslant 18$,矛盾。

K_5 和 $K_{3,3}$分别记为 $K^{(1)}$和 $K^{(2)}$图。

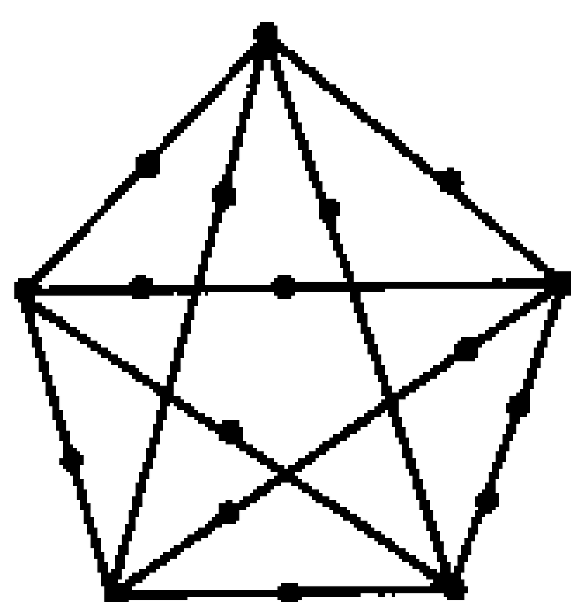
定义 4.3.1 在 $K^{(1)}$和 $K^{(2)}$图上任意增加一些度为 2 的结点之后得到的图称为 $K^{(1)}$型和 $K^{(2)}$型图,统称为 K 型图,如图 4.7 所示。

因为 K 型图里的这些度为 2 的结点不会处于两条边的交点上,因此 $K^{(1)}$型和 $K^{(2)}$型图都是非平面图。

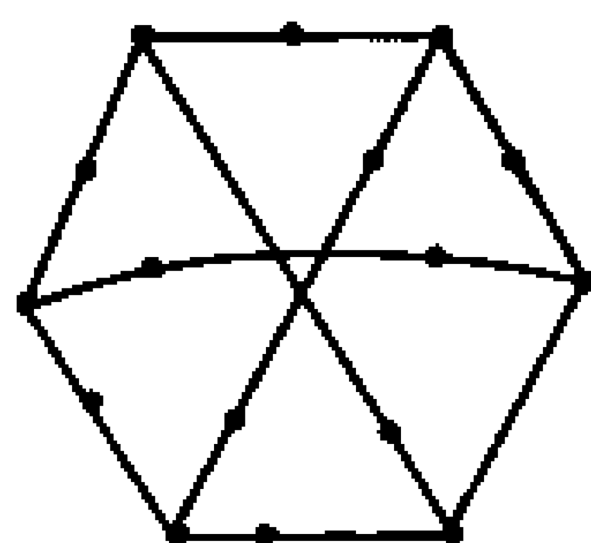
库拉图斯基(Kuratowski)给出了区分可平面图与非平面图的一个著名定理。

定理 4.3.3 G 是可平面图的充要条件是 G 不存在 K 型子图。

定理的必要性容易证明。假定 G 存在 K 型子图,因为 K 型子图不可平面,所以 G 是非平面图。其充分性的证明需占较长的篇幅,在此从略。



$K^{(1)}$型



$K^{(2)}$型

图 4.7

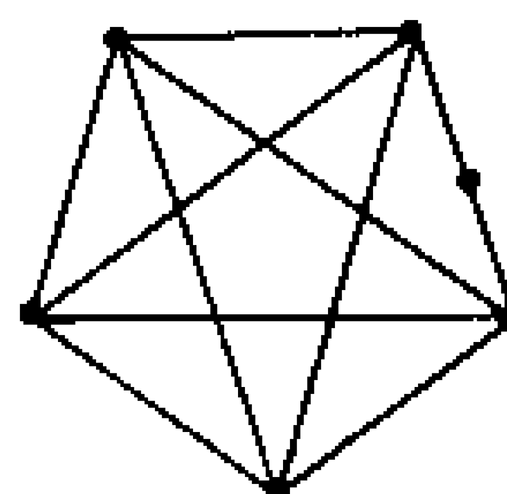


图 4.8

例 4.3.2 K_6 图既含有 $K^{(1)}$型子图,也含有 $K^{(2)}$型子图。比如图 4.8 就是它的 $K^{(1)}$型子图。

库拉图斯基定理在理论上具有重要价值,但是在实际中,用它确定一个图 G 是否存在 K 型子图将是非常困难的。因此,必须探索实用的平面性算法。

4.4 图的平面性检测

判定一个图是否可平面的,首先应该做一些预处理工作。

1. 如果 G 是非连通的,则分别检测每一个连通支。仅当所有的连通支都是可平面的,G 就是可平面的。

2. 如果 G 中存在割点 v(参见 6.1),这时可把图 G 从割点处分离,构成若干个不含割点的连通子图,或称块,然后检测每一块。显然 G 是可平面的,当且仅当每一块都是可平面的。

3. 移去自环。

4. 移去度为 2 的结点 v_i 及其所关联的边，而在它的两个邻点 v_j，v_k 之间加入边(v_j，v_k)，显然原图是可平面的，当且仅当新图是可平面的。

5. 移去重边。

反复运用 4 和 5。最后，如果

a. $m<9$ 或 $n<5$，则 G 是可平面的。

b. $m>3n-6$，则 G 是非平面的。

c. 不满足 a 和 b，需要进一步测试。

例 4.4.1 判定图 4.9 的可平面性。

解：运用前述判定规则，G 有两个割点 v_1，v_2；可分成 3 个块分别检测，最后或 $n<5$，或 $m<9$，因此 G 是可平面的。

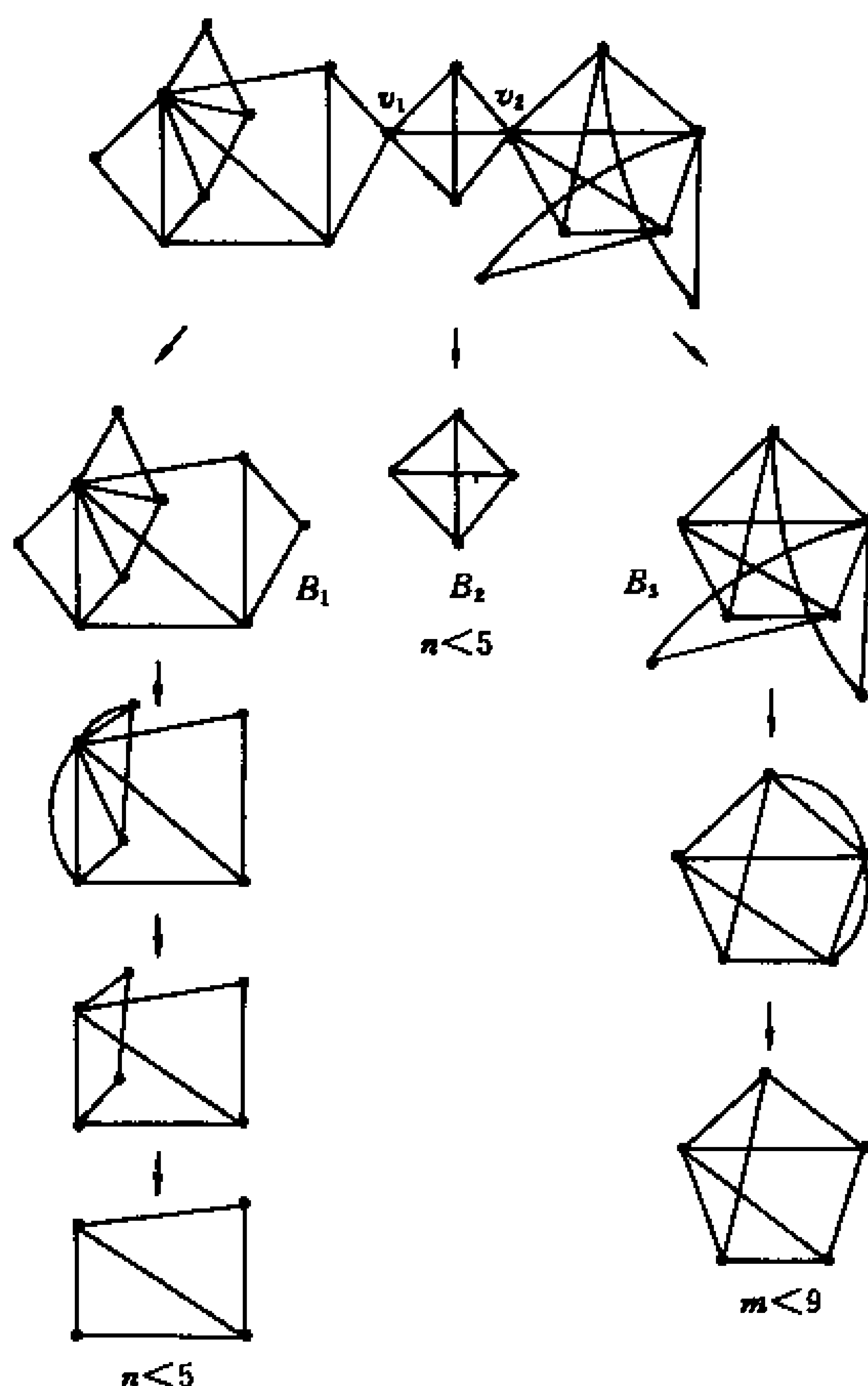


图 4.9

前面已述，如果不满足条件 a 和 b，G 的平面性不能断定，需要进行进一步检测。至今已经提出了不少平面性测试算法，1964 年 Demoucron，Malgrange 和 Pertuiset 提出了一个较为简单但有效的算法，其后，Hopcroft 和 Tarjan 又最早给出了一个复杂性为 $O(n)$ 的算法，由于该算法的解释与证明所占篇幅太长，所以在这里我们仅介绍 DMP 算法。

设 H 是 G 的可平面子图，如果在 $G-H$ 中存在另一个 G 的平面子图 B，且 B 与 H

有 2 个以上共同结点，则称 B 是 G 中 H 的片，片 B 与 H 的公共点称为片 B 的附着点。

片是 DMP 算法中一个重要的概念。

例 4.4.2 图 4.10(a)中，令 H 是回路(v_1,v_2,v_3,v_4)，它可以有三个片：$B_1=\{(v_2,v_4)\}$，附着点为 v_2,v_4；$B_2=\{(v_1,v_3)\}$，附着点是 v_1,v_3；$B_3=\{(v_1,v_5),(v_2,v_5),(v_3,v_5),(v_4,v_5)\}$，附着点是 v_1,v_2,v_3,v_4。

设 $\tilde{H}$ 是 G 的子图 H 的一个平面嵌入，令 B 是关于 H 的任一片，显然只有当 B 的所有附着点都在 $\tilde{H}$ 里某个面 f 的边界上，B 才能画在 $\tilde{H}$ 的一个面内。比如图 4.10(b)，$\tilde{H}$ 中有两个面的边界都包含了 B_1 的全部附着点，所以片$\{(v_2,v_4)\}$可以如图(b)画在内部面上(也可以画在外部面里)，得到新的子图 H_1 的平面嵌入 $\tilde{H}$，这时只有外部面的边界包含了片 B_2 的全部附着点，因此 B_2 只能画在外部面内。这样又得到子图 H_2 的平面嵌入 $\tilde{H}_2$，这时 $\tilde{H}_2$ 里不存在一个面，它的边界包含了 B_3 的全部附着点，B_3 就不可能平面嵌入到 $\tilde{H}_2$ 的某个面内。所以 G 是不可平面的。为叙述方便，我们记 $F(B,\tilde{H})$ 为片 B 可平面嵌入的 $\tilde{H}$ 的面的集合

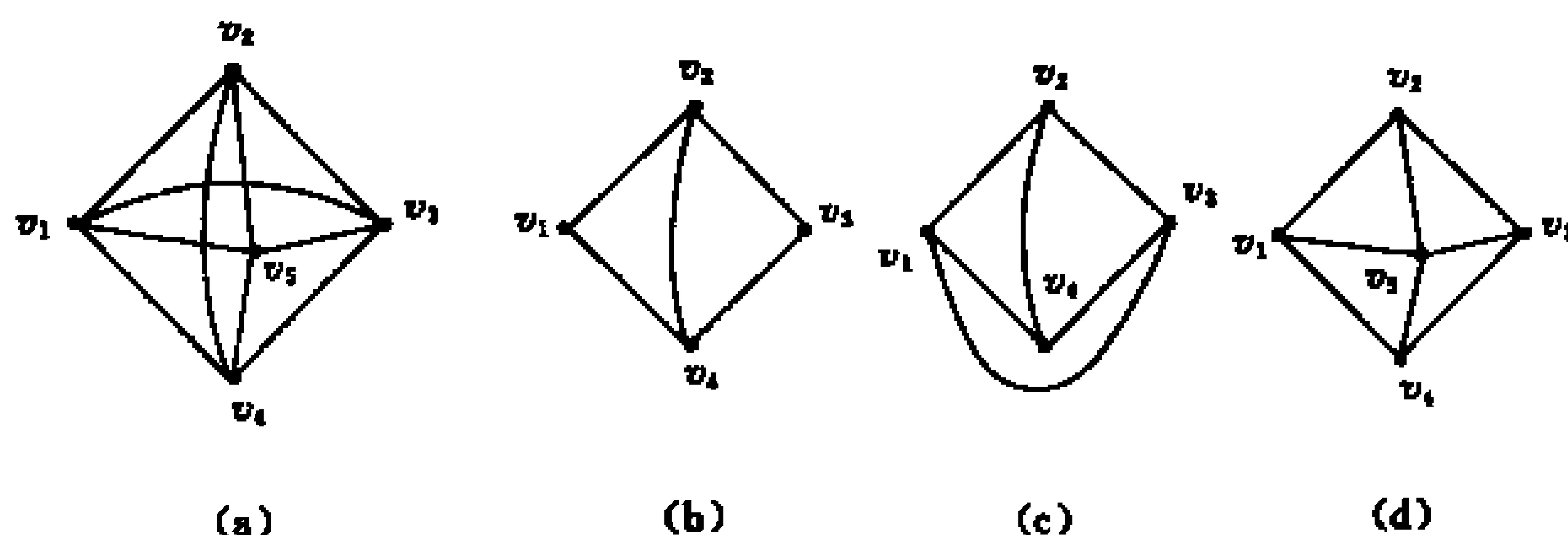


图 4.10

DMP 算法描述如下：

1. 找 G 的一个回路 C。
2. i←1。
3. G_1←C，$\tilde{G}_1$←C。
4. f←2。
5. EMBEDDABLE←true。
6. While f≠m−n+2 and EMBEDDABLE do
   begin
7. 找 G 关于 G_i 的每一个片 B。
8. 对每一个片 B，求 F(B，$\tilde{G}_i$)。
9. 若对某一个 B，F(B，$\tilde{G}_i$)=Φ，则
      EMBEDDABLE←false；G 是非平面图，结束。
10. 若 EMBEDDABLE 则
    begin
11. if 对某个 B，|F(B，$\tilde{G}_i$)|=1 then F←F(B，$\tilde{G}_i$)，
    else 令 B 是任何一个片，且 F 是满足 F∈F(B，$\tilde{G}_i$)的任何一个面。

12. 找一条路径 P_i B,P_i 的两端点是 G_i 的结点。

13. $G_{i+1} \leftarrow G_i + P$。

14. 将 P_i 画到 $\tilde{G}_i$ 的面 F 内,得到 G_{i+1} 的平面嵌入 $\tilde{G}_{i+1}$。

15. $i \leftarrow i+1$。

16. $f \leftarrow f+1$。

17. 若 $f=m-n+2$,则 G 可平面。

    end

  end。

DMP 算法在不断地寻找满足 G_i, G_{i+1} 的图 $G_1, G_2, \cdots$,并且求它们的平面嵌入 $\tilde{G}_1, \tilde{G}_2, \cdots$,如果 G 是可平面的,算法将在 $\tilde{G}_{m-n+1}$ 时结束,即获得了 G 的平面嵌入。如果 G 是非平面的,则算法在发现某个片 $B, F(B, \tilde{G}_i)=\Phi$ 时结束。很明显,G 是可平面的必要条件就是关于 G_i 的每个片 B,都有 $F(B, \tilde{G}_i) \neq \Phi$。

算法首先找 G 的一个回路 G_1,因为 G 是块,所以必含有回路,而且它是可平面的。如果尚未检测到 $\tilde{G}_i$ 的一个片 B,使 $F(B, \tilde{G}_i)=\Phi$ 时,布尔变量 EMBEDDABLE 一直为真,否则为假,算法将以 G 为非平面图结束。变元 f 用来记录 $\tilde{G}_i$ 的面的数目,初值为 2,并随执行 While 语句而增加,同时,每执行一次 While 语句,将从 $\tilde{G}_i$ 得到 $\tilde{G}_{i+1}$,它是通过下述过程实现的:算法第七、八行分别找 G 关于 G_i 所有的片以及每个片的 $F(B, \tilde{G}_i)$。如果有一片只能画在某个面 F 内,就在 F 内部画一条包含 B 的两个附着点的路径 P_i,从而构成 $\tilde{G}_{i+1}$;如果没有这样的片存在,则 P_i 可以是任何一个片中包含其两个附着点的一条边,在以上两种情况下,P_i 都把某个面 F 分成两部分,从而使 f 增加 1。当然,若 G 是可平面的,$\tilde{G}$ 一定有 $m-n+2$ 个面,这时算法结束。

当然在算法实现时,每个 $\tilde{G}_i$ 可以用它的面的集合 $\{F_i\}$ 表示,其中每个 F_i 用结点的有序集,比如顺时针方向,标志它的界,从而使 P_i 的添入过程变得方便。

定理 4.4.1 DMP 算法是正确的。

证明:我们只需证明:如果 G 是可平面的,$G_i \subseteq G$,$\tilde{G}_i$ 是 G_i 的平面嵌入,那么必有 $\tilde{G}_i \subseteq \tilde{G}$。采用归纳法,若 G 是可平面的,显然 $\tilde{G}_1 \subseteq \tilde{G}$。假定对某个 i,$\tilde{G}_i \subseteq \tilde{G}$,我们将证明 $\tilde{G}_{i+1} \subseteq \tilde{G}$。令 B 和 F 是算法第 11 行所定义的,如果 $|F(B, \tilde{G}_i)|=1$,那么由算法所构造的 $\tilde{G}_{i+1}$ 一定满足 $\tilde{G}_{i+1} \subseteq \tilde{G}$。如果 $|F(B, \tilde{G}_i)|>1$,有可能片 B 不画在 $\tilde{G}$ 的某个面 F 内,而画在另一个面 F' 里。由于 G 是一个块,它没有割点,所以关于 G_i 的每个片都至少有 2 个附着点,并且它只能画在 2 个面内,这样每一个片的附着点一定在面 F 和 F' 的公共边界上,这个片既可以画在 F 内,也可以画在 F' 内。因此,存在 G 的两个平面嵌入,一个是片 B 画在 $\tilde{G}$ 的面 F 里,另一个是画在 $\tilde{G}$ 的面 F' 里。这样由算法构造的 $\tilde{G}_{i+1}$ 是 G 的子图,即是 G 的某个子图的平面嵌入。

DMP 算法的计算复杂性虽然不如 H.T 等算法,但它依然是多项式时间的。在算法实现时还需要注意一些特点,比如在加入一条路 P_i 之后,G_i 除了 P_i 所在的片之外,其于的片仍然都是 $\tilde{G}_{i+1}$ 的片,类似的特点可以帮助提高算法的效率。

例 4.4.3 DMP 算法对图 4.11(a)的平面性测试过程如下:

$\tilde{G}_i$	f	片 B	$F(B,\tilde{G}_i)$	B	F	P_i
$\tilde{G}_1$	2	B_1	$\{F_1,F_2\}$			
		B_2	$\{F_1,F_2\}$			
		B_3	$\{F_1,F_2\}$			
		B_4	$\{F_1,F_2\}$			
		B_5	$\{F_1,F_2\}$	B_1	F_1	(1,3)
$\tilde{G}_2$	3	B_2	$\{F_2,F_3\}$			
		B_3	$\{F_2,F_3\}$			
		B_4	$\{F_2,F_3\}$			
		B_5	$\{F_2\}$	B_5	F_2	(2,7,5)
$\tilde{G}_3$	4	B_2	$\{F_3\}$			
		B_3	$\{F_3,F_6\}$			
		B_4	$\{F_3\}$			
		B_6	$\{F_5\}$			
		B_7	$\{F_5,F_8\}$	B_2	F_3	(1,4)
$\tilde{G}_4$	5	B_3	$\{F_6\}$			
		B_4	$\{F_7\}$			
		B_6	$\{F_5\}$			
		B_7	$\{F_5,F_6\}$	B_3	F_6	(3,5)
$\tilde{G}_5$	6	B_4	$\{F_7\}$			
		B_6	$\{F_5\}$			
		B_7	$\{F_5,F_9\}$	B_4	F_7	(4,6)
$\tilde{G}_6$	7	B_6	$\{F_5\}$			
		B_7	$\{F_5,F_9\}$	B_6	F_5	(6,7)
$\tilde{G}_7$	8	B_7	$\{F_9\}$	B_7	F_9	(2,8,5)
$\tilde{G}_8$	9	B_8	$\{F_{15}\}$	B_8	F_{15}	(7,8)
$\tilde{G}_9$	10	$f=m-n+2$ 结束				

表中：$B_1=\{(1,3)\}$，$B_2=\{(1,4)\}$，$B_3=\{(3,5)\}$，$B_4=\{(4,6)\}$，$B_5=\{(7,8),(7,2),(7,5),(7,6),(8,2),(8,5)\}$，$B_6=\{(6,7)\}$，$B_7=\{(8,2),(8,5),(8,7)\}$，$B_8=\{(7,8)\}$。

例 4.4.4 DMP 算法对图 4.12 的测试过程如下：

$\tilde{G}_i$	f	片 B	$F(B,\tilde{G}_i)$	B	F	P_i
$\tilde{G}_1$	2	B_1	$\{F_1,F_2\}$			
		B_2	$\{F_1,F_2\}$			
		B_3	$\{F_1,F_2\}$	B_1	F_2	(1,3)
$\tilde{G}_2$	3	B_2	$\{F_1\}$			
		B_3	$\{F_1\}$	B_2	F_1	(2,4)
$\tilde{G}_3$	4	B_3	Φ			

表中：$B_1=\{(1,3)\}$，$B_2=\{(2,4)\}$，$B_3=\{(1,5),(2,5),(3,5),(4,5)\}$。

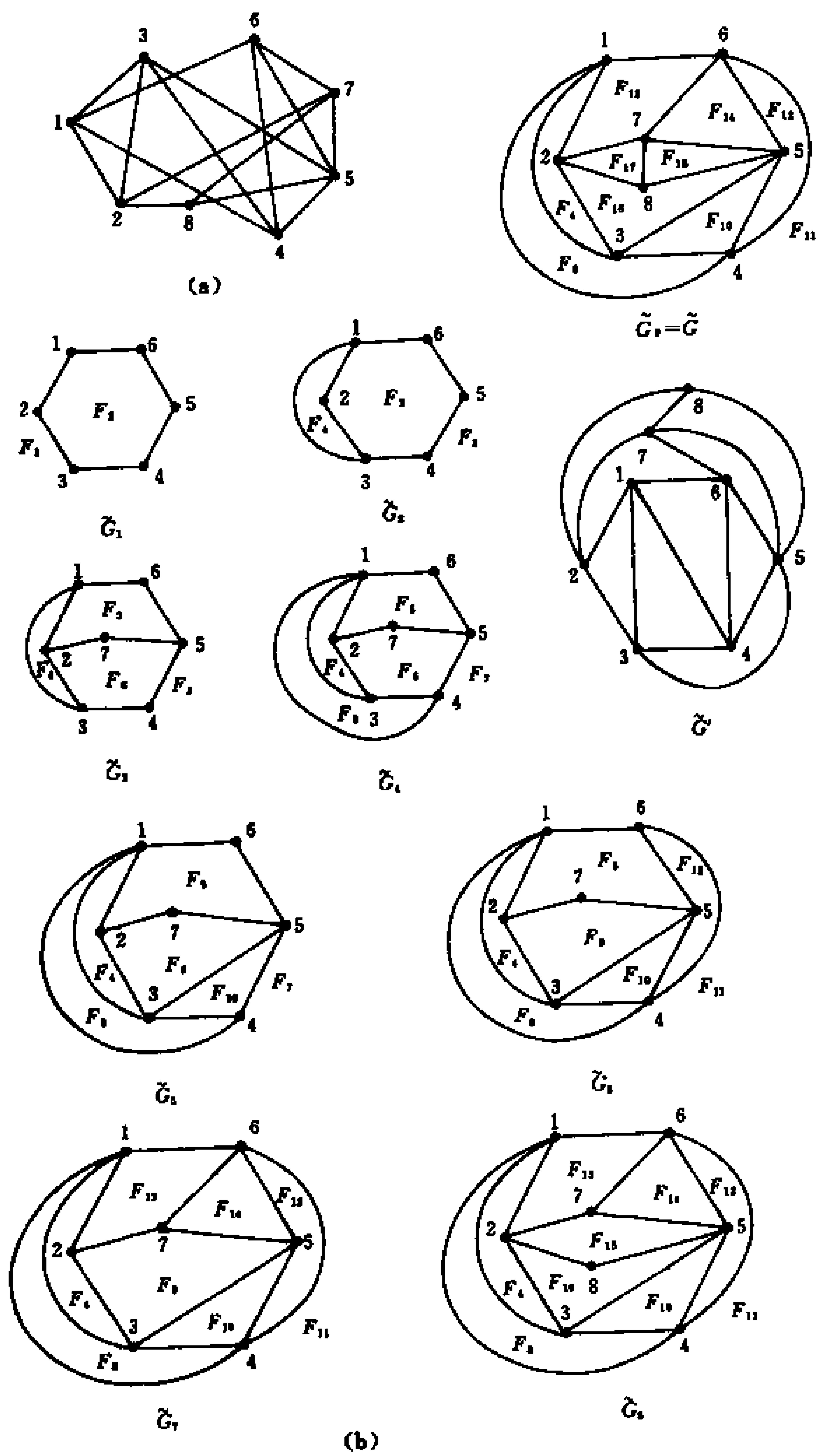


图 4.11

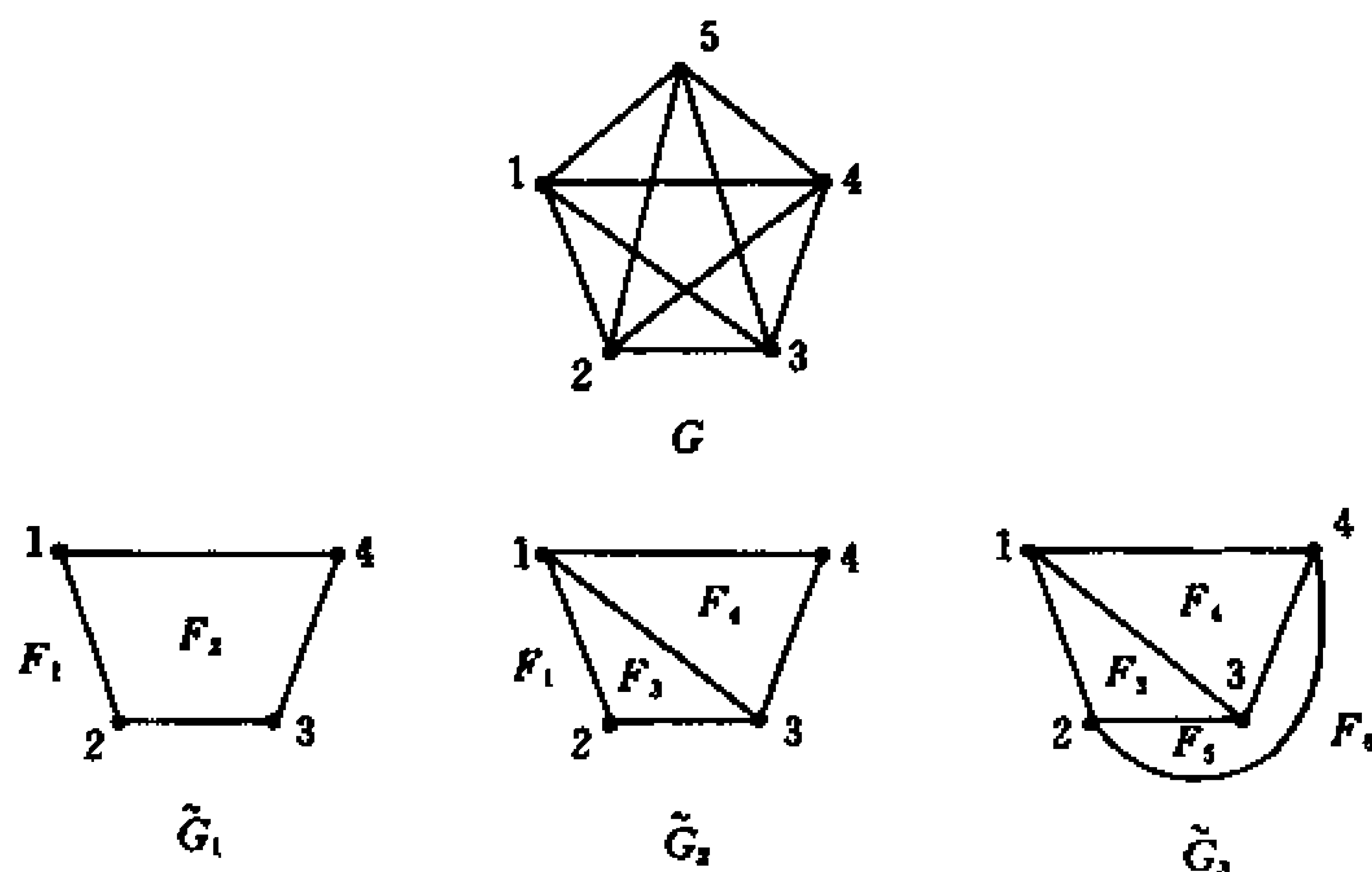


图 4.12

4.5 对 偶 图

给定一个平面图 G,它的每个域的边界便得到了确定。这样,由图 G 可以导出另一个图 G^*,称为图 G 的对偶图。

定义 4.5.1 满足下列条件的图 G^* 称为 G 的对偶图。

1. G 中每个确定的域 f_i 内设置一个结点 v_i^*。
2. 对域 f_i 和 f_j 的共同边界 e_k,有一条边 $e_k^*=(v_i^*,v_j^*)\in E(G^*)$,并与 e_k 相交一次。
3. 若 e_k 处于域 f_i 之内,则 v_i^* 有一自环 e_k^* 与 e_k 相交一次。

很明显,这个定义本身就是求图 G 对偶图 G^* 的方法,它亦称为 D(drawing)过程。

例 4.5.1 图 4.13(a)、(b)的对偶图如虚线边所示。

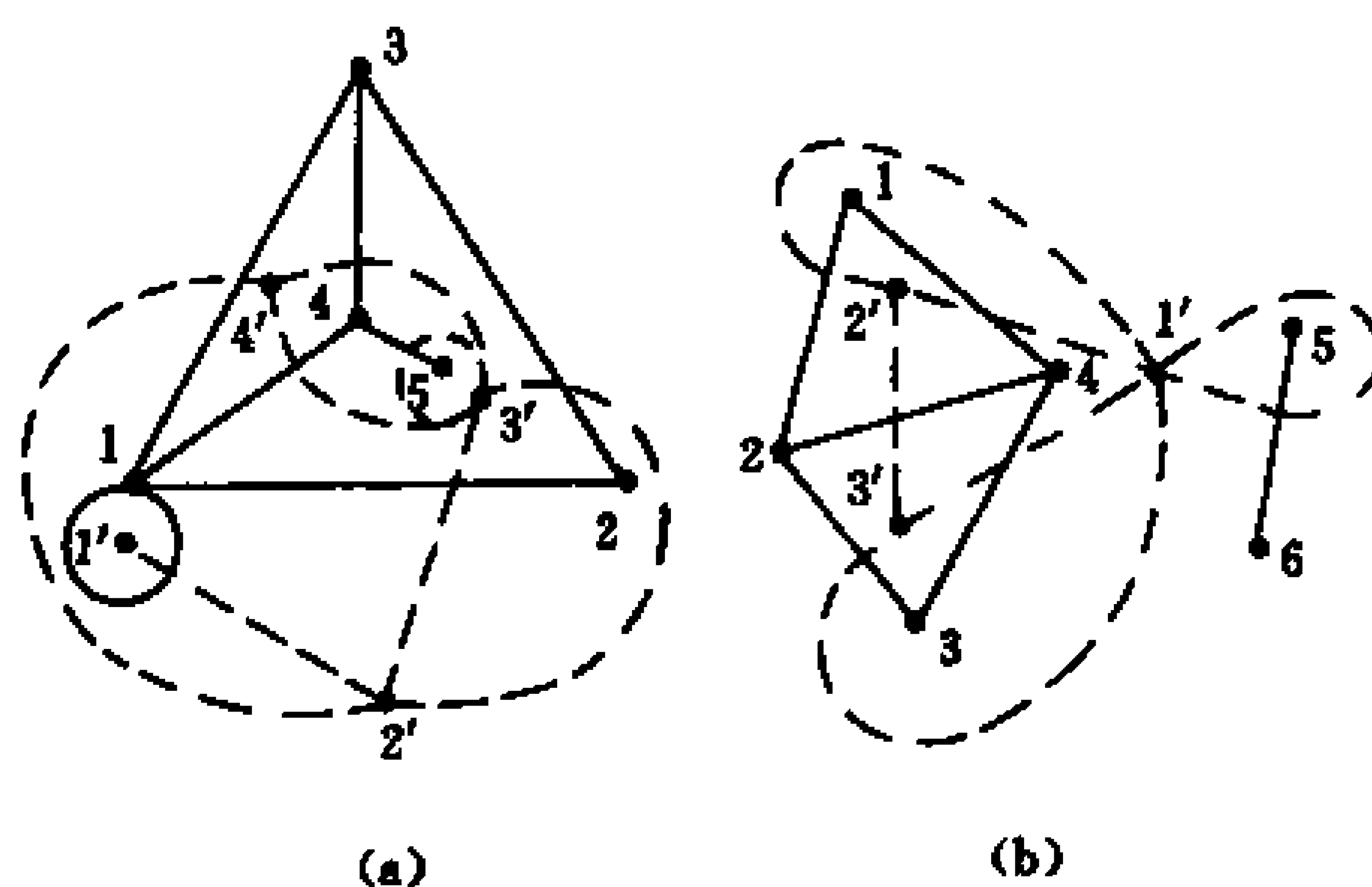


图 4.13

G 的对偶图 G^* 具有如下性质:

性质 4.5.1 如果 G 是平面图,G 一定有对偶图 G^*,而且 G^* 是唯一的。

由 D 过程即可得证。

性质 4.5.2 G^*是连通图。

在平面图G里，每个域f都存在相邻的域，而且对G的任何部分域来说，都存在与它们之中某个域相邻的域。这样由对偶图的定义可知，G^*连通。

性质 4.5.3 若G是平面连通图，那么$(G^*)^*=G$。

性质 4.5.4 平面连通图G与其对偶图G^*的结点、边和域之间存在如下对应关系

$$m=m^*,\quad n=d^*,\quad d=n^*。$$

性质 4.5.5 设C是平面图G的一个初级回路，S^*是G^*中与C的各边e_i对应的e_i^*的集合，那么S^*是G^*的一个割集。

证明：C把G的域分成了两部分，因此$E(G^*)-S^*$把G^*的结点分成不连通的两部分，由性质 4.5.2，G^*这两部分分别是连通的，因此S^*是G^*的一个割集。

定理 4.5.1 G有对偶图的充要条件是G为平面图。

证明：充分性直接由性质 4.5.1 得证。现证其必要性，即非平面图没有对偶图。由库拉图斯基定理，非平面图一定含有$K^{(1)}$或$K^{(2)}$型子图；而$K^{(1)}$、$K^{(2)}$型子图是$K^{(1)}$和$K^{(2)}$图中增加了一些度为 2 的结点，因此如果$K^{(1)}$、$K^{(2)}$图没有对偶图，那么$K^{(1)}$、$K^{(2)}$型，进而非平面图也没有对偶图。下面我们分别进行讨论。

(1) 对$K^{(1)}$图，$m=10,n=5,d\geqslant7$，假定$K^{(1)}$有对偶图，由性质 4.5.4，$m^*=10,n^*\geqslant7$。由于$K^{(1)}$中没有自环和重边，故$d(v_i^*)\geqslant3$，

$$\sum d(v_i^*)\geqslant 3\times 7>2m^*,$$

因此$K^{(1)}$没有对偶图。

(2) 对$K^{(2)}$图，$m=9,n=6,d\geqslant5$。假定$K^{(2)}$有对偶图。由性质 4.5.4，$m^*=9,n^*\geqslant5$。由于$K^{(2)}$中每个域的边界数至少为 4，故$d(v_i^*)\geqslant4$，

$$\sum d(v_i^*)\geqslant 4\times 5>2m^*,$$

因此$K^{(2)}$没有对偶图。

综上定理得证

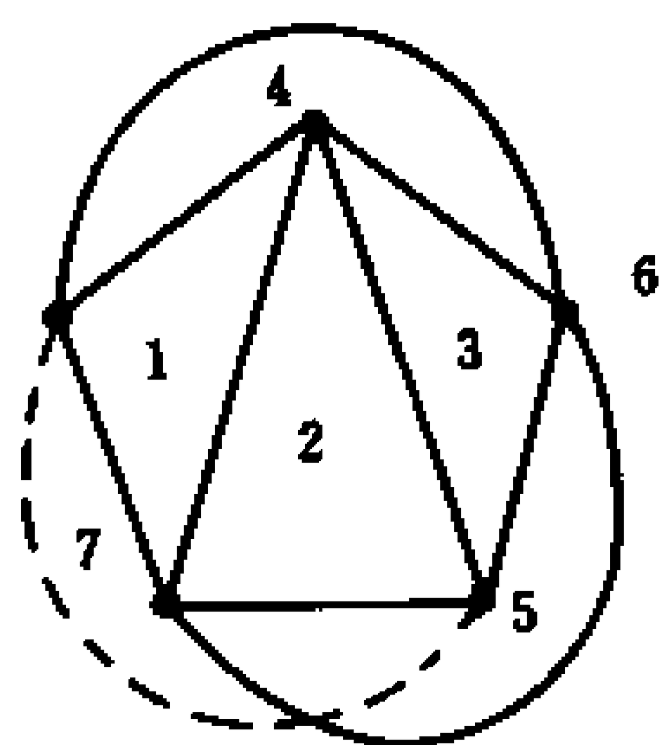


图 4.14

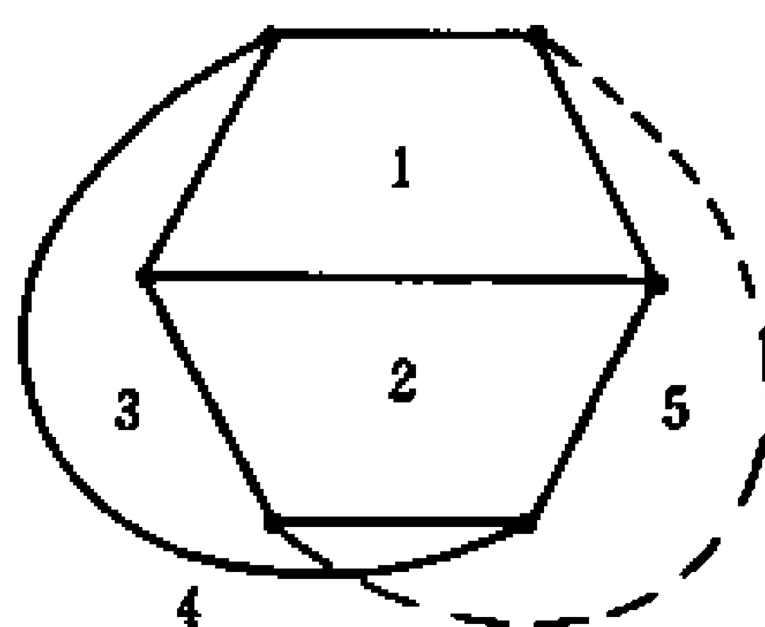


图 4.15

利用对偶原理，有时可以使问题变得十分简单。

例 4.5.2 图 4.16 是一所房子的俯视图，设每一面墙都有一个门。问能否从某个房间开始过每扇门一次最后返回。

解：做G的对偶图G^*，原问题就转化为G^*是否存在欧拉回路。显见与G的域f_1和

f_2 所对应的 G^* 的结点 v_1^* 和 v_2^* 的度为奇，因此不存在欧拉回路

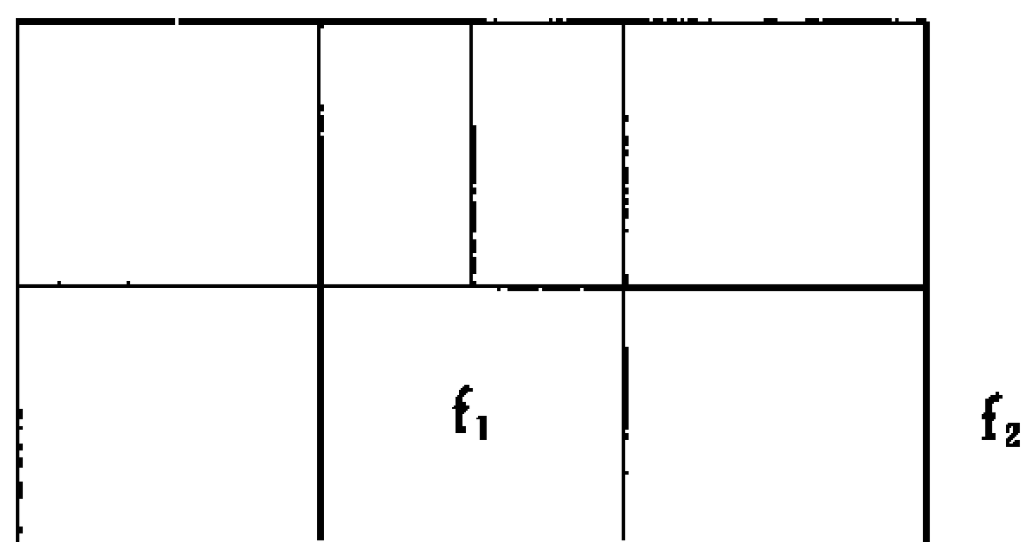


图 4.16

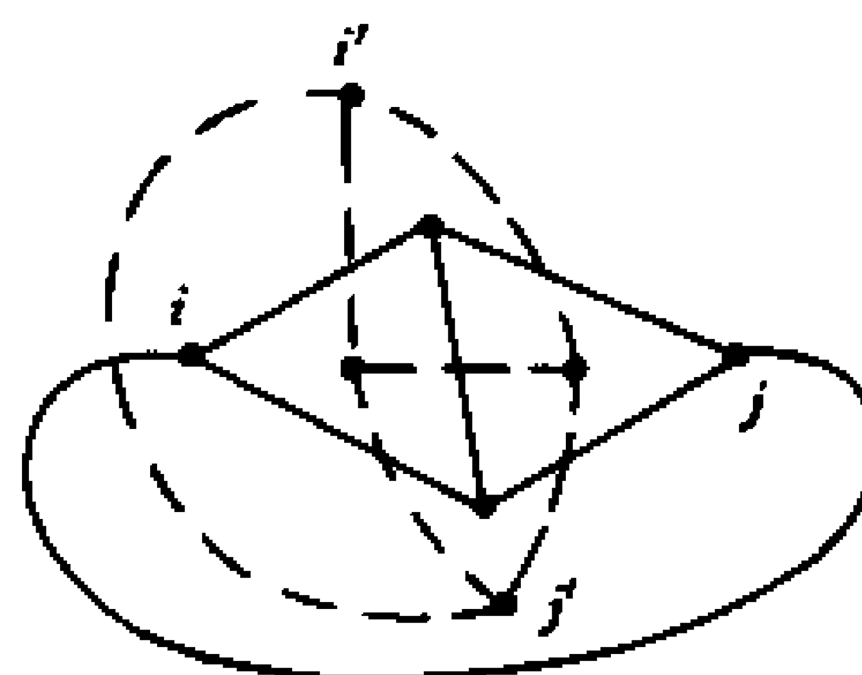


图 4.17

例 4.5.3 设 i 和 j 是平面连通图无限域边界上的两个结点，求 G 中分离 i 和 j 的所有割集。

解：在无限域中添入边 (i,j)，得到 G_1，如图 4.17 所示，作 G_1 的对偶 G_1^*，则 G_1^* 中除 (i',j') 之外的从 i' 到 j' 的初级道路所对应的 G 的诸边都构成了 G 中分离 i 和 j 的割集。

对偶图还广泛用于平面图域的染色上。

一张彩色地图，通常使用 4 种以上的颜色标明各个国家的疆域。人们所熟知的著名的"四色猜想"，就是推断对任何一张地图，或者说任何一个平面图，只需 4 种不同的颜色就可以对它的域进行染色，满足相邻的域染以不同的颜色。这个猜想至今还没有用数学方法获得证明。但是增加一种颜色，即平面图域的 5 着色却是容易证明的。

定理 4.5.2 每一个平面图 G 都是 5－可着色的。

证明：作 G 的对偶图 G^*，命题转为证 G^* 的结点 5－可着色。当然 G^* 也是可平面图。由于自环和重边不影响点染色，所以可移去 G^* 中的自环、重边，得到简单图 G_0。命题又转化为任意简单平面图 G_0 可以结点 5 着色。以下对 G_0 的结点进行归纳证明，当 $n\leqslant 5$ 时，结论显然；设 $n-1$ 时成立，则结点数为 n 时，由于 G_0 是简单图，由定理 4.2.2，G_0 中存在结点 v，$d(v)<6$。移去 v 后得到 G_0'，由假设条件，G_0' 的结点可 5－着色，着好色之后，再把 v 放回。由于 G_0 是平面图，v 一定是在 G_0' 的某个域里面。如果 $d(v)\leqslant 4$，或者 $d(v)=5$，同时 v 的邻接点没有用完 5 种颜色，那么 G_0 的点可以 5 着色。而如果 v 的邻接点恰好用了 5 种颜色，比如 $c_1\sim c_5$。设用 c_i 着色的结点为 v_i，如图 4.18所示。

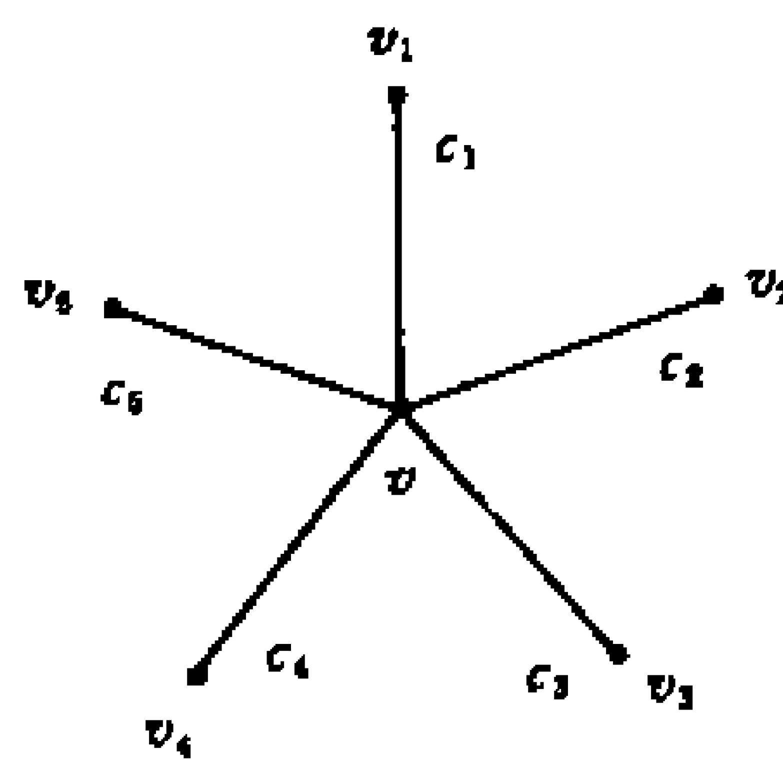


图 4.18

令 G_{13} 是 $G_0'=G_0-v$ 的一个子图，它是由 c_1 和 c_3 着色的结点导出。若 v_1 和 v_3 分属于 G_{13} 不同的连通支，则将 v_1 所在连通支各结点 c_1、c_3 颜色对换，v 可着以 c_1，得到 G_0 的一个 5 着色。如果 v_1 和 v_3 属于 G_{13} 同一个连通支，那么一定存在 v_1 到 v_3 的结点交替着 c_1、c_3 颜色的道路 P，加上边 (v,v_1)，(v,v_3) 构成一个封闭回路，它把 v_2 与 v_4、v_5 分隔在不同的区域。这时在任何情况下，都不会存在由 c_2 和 c_4 交替对结点染色的连接 v_2 和 v_4 的道路 P'。否则与 G_0 是平面图矛盾。这也就是说，在 G_0-v 的子图 G_{24} 中，v_2 和 v_4 分属于不同的支。将 v_2 所在连通支各结点的 c_2、c_4 颜色对换，此时 v_2 着以 c_4，于是可令 v 着以 c_2 从而使 G_0 可以 5 着色。

采用五色定理的证明方法是无法证明四色猜想的。关于四色问题，下面介绍一些有关的结论。

定理 4.5.3 如果平面图 G 有哈密顿回路，则四色猜想成立。

这个结论已在 2.4 节中给出。

定理 4.5.4 若任何一个 3－正则平面图的域可四着色，则任何平面图的域也可以四着色。

证明：3－正则平面图是指每个结点的度都是 3 的平面图。任何一个平面图 G，如果存在度为 1 的结点 v，则它一定处于某个域的内部，移去 v 并不影响这个域的染色。如果存在度为 2 的结点 v_i，删去 v_i 及其关联的边 (v_i,v_j)，(v_i,v_k)，同时增加一条边 (v_j,v_k)，也不会影响域的染色。如果存在结点 v，满足 $d(v)\geqslant 4$。它关联于边 $e_1,e_2,\cdots,e_k$，设这些边依次环绕于 v。我们对应每一条 e_i 构造一个新结点 v_i，然后移去 v，并加入新的边 (v_1,v_2)，(v_2,v_3)，…，(v_k,v_1)，这样新加入的每一个结点的度也是 3，如图 4.19 所示。这时图 G 转化为 3－正则平面图 G'。由已知条件 G' 的域可四着色，再把由 $v_1,v_2,\cdots,v_k$ 作为边界点的域收缩，最后还原成一个结点 v，那么 G' 的域染色仍然适用于 G。

基于上述两个定理，Tait 曾提出过一个猜想。

猜想：任何一个 3－正则的平面图都有哈密顿回路。

显然，如果这个猜想成立，那么四色猜想也便获得了证明。后来托特(Tutte)最早给出了一个反例，推翻了这个猜想。托特的反例是这样构思的。

首先构造一个 3－正则平面图 G_1，如图 4.20。可以证明 G_1 的 H 回路必不同时过 a，b 两边。否则，由对称性，如果 H－回路经过边(1,2)，则一定过(2,7)，(7,8)。这样在图的下半部，它一定要经过边(3,4)和(6,10)。这时，若经过结点 5，就不经过结点 9，反之亦然。因此结论得证。

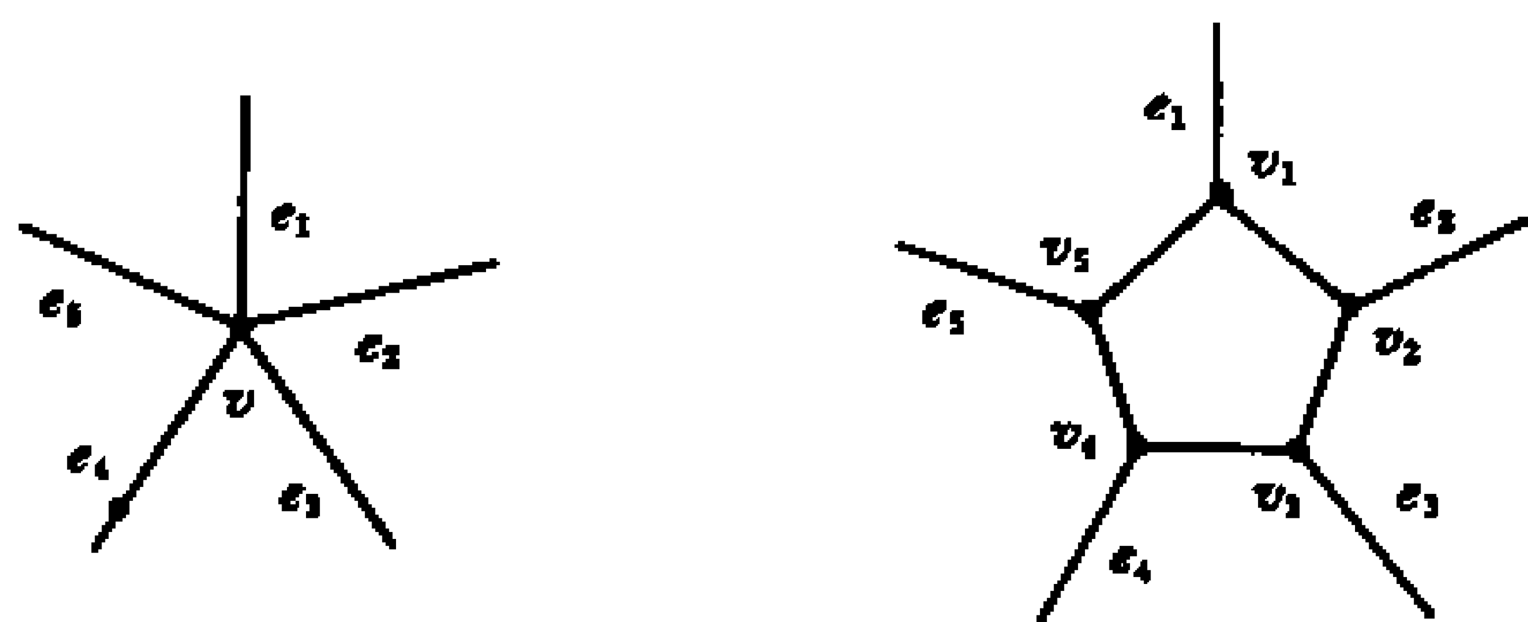


图 4.19

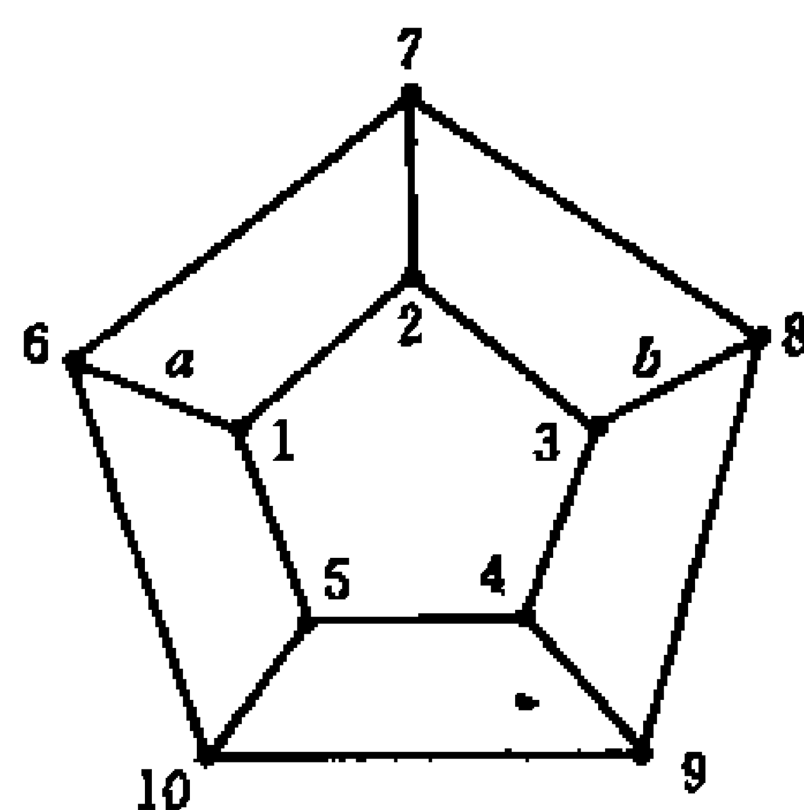


图 4.20

这时再把结点 6 和 8 放大，分别构成一个域，得到图 G_2，它也是一个 3－正则平面图。同样可证 G_2 的 H－回路必不同时经过边 c 和 d。如若不然，它亦必同时经过 a，b。由前面结论这是不可能的。

这样在 G_2 中再在边 c 和 d 上各增设一个结点 u 和 v，并添加边 (u,v)。得到 3－正则平面图 G_3。我们又可以断言，如果 G_3 中有 H 回路，则必经过边 (u,v)，因为不然的话，它必同时过 G_2 中的 c，d，因而必同过 a，b。矛盾。

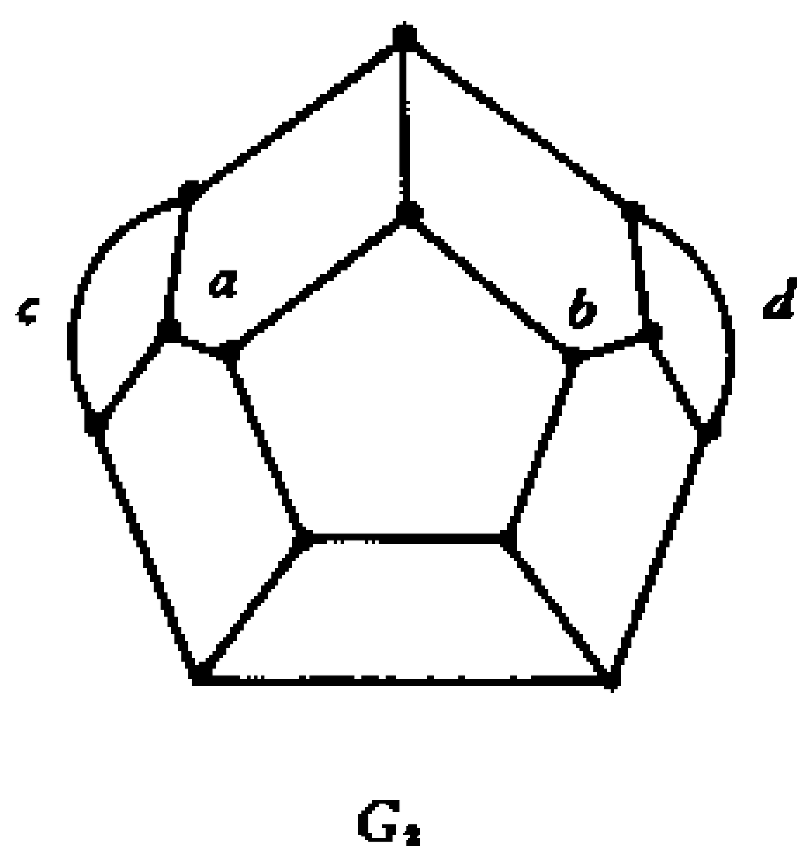


图 4.21

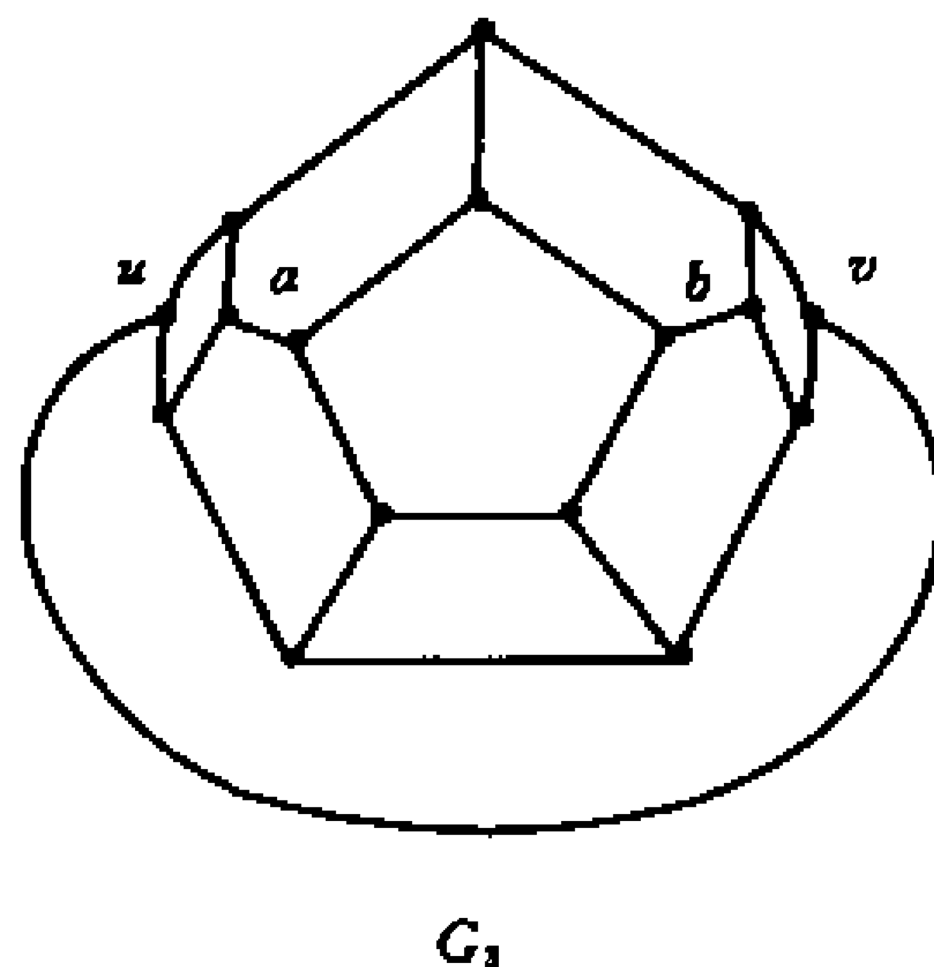


图 4.22

在G_3中移去结点v，增加3个度为1的结点x,y,z，并保留与v关联的边，构成G_4，然后由三个与G_4同构的平面图搭接，组成一个更大的图，并移去搭接时出现的度为2的结点，得到G。如图4.24。G也是3－正则平面图。如前所证，如果G中有H回路，它必定经过每一条边e，这样就一定重复通过结点z，矛盾。因此G中不存在H回路。

在托特之后，又不断提出了一些不满足Tait猜想的图例，这些图包含的结点数和边数比托特的反例更少。由于四色猜想至今没获得数学证明，所以它仍然布满着神秘的色彩。

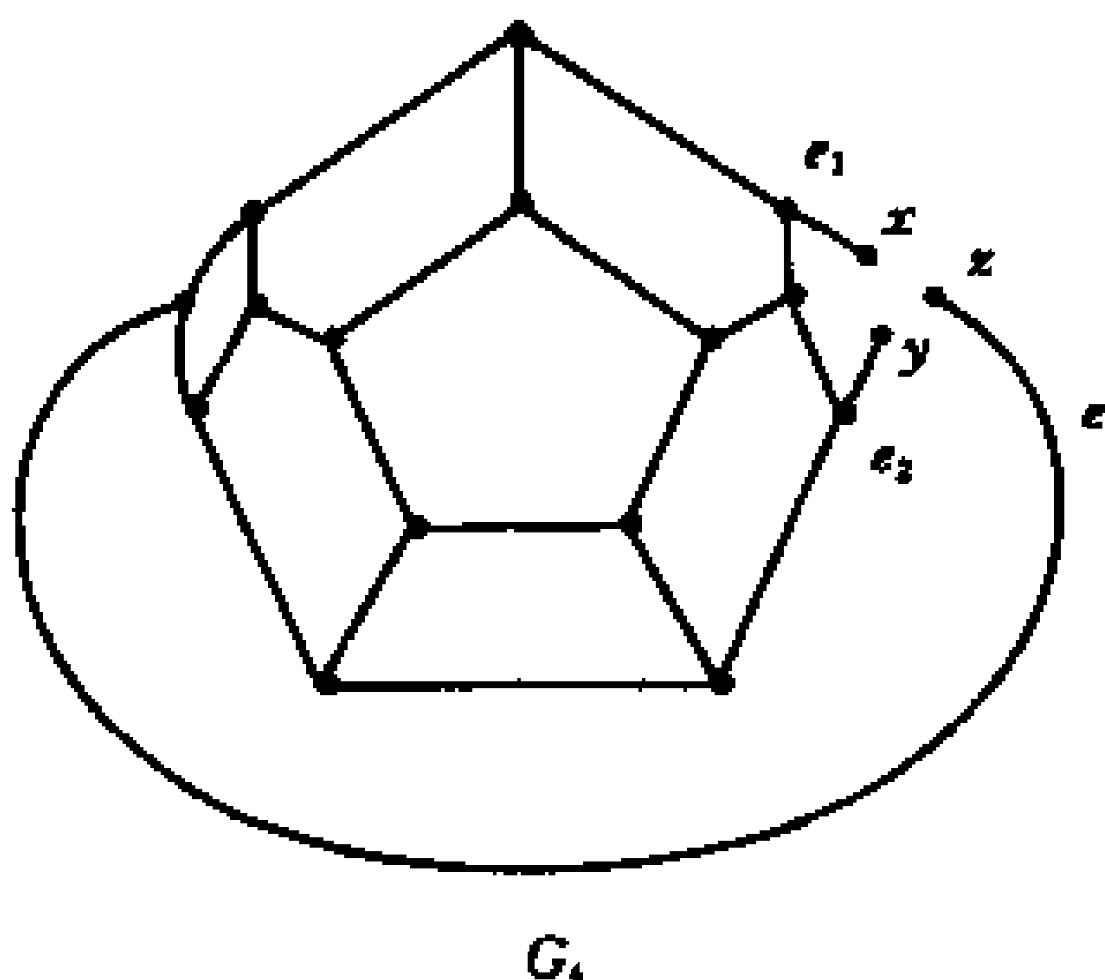


图 4.23

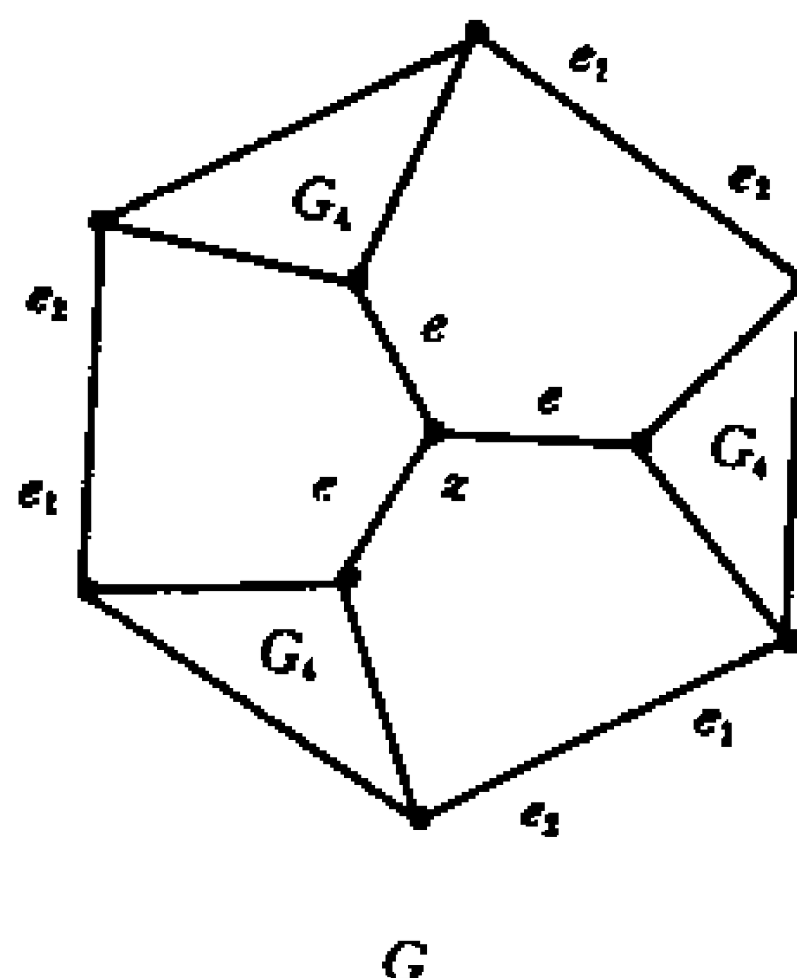


图 4.24

4.6 色数与色数多项式

上节讨论了平面图的域着色问题，它是通过对其对偶图的结点着色来实现的。实际上图G同样存在着结点着色与边着色问题。

例4.6.1 六种货物要存放在仓库里，其中一些货不能放在同一个仓库，它们之间的关系如图4.25所示，其中$e=(i,j)$表示i与j不能存放在同一库房。如果A放在1号库，则C、D只能分别放在2、3号库，那么需要的库房数至少是多少呢？在这时，B,E,F可以分别放在1、2、3号库。也就是说有3个库房是能够满足要求的。

使用图论的术语，这就是对图 G 的结点着色，满足相邻的结点着以不同的颜色。

定义 4.6.1 给定图 G，满足相邻结点着以不同颜色的最少颜色数目称为 G 的色数，记为 $\gamma(G)$。

定义 4.6.2 给定图 G，满足相邻边着以不同颜色的最少颜色数目称为 G 的边色数，记为 $\beta(G)$。

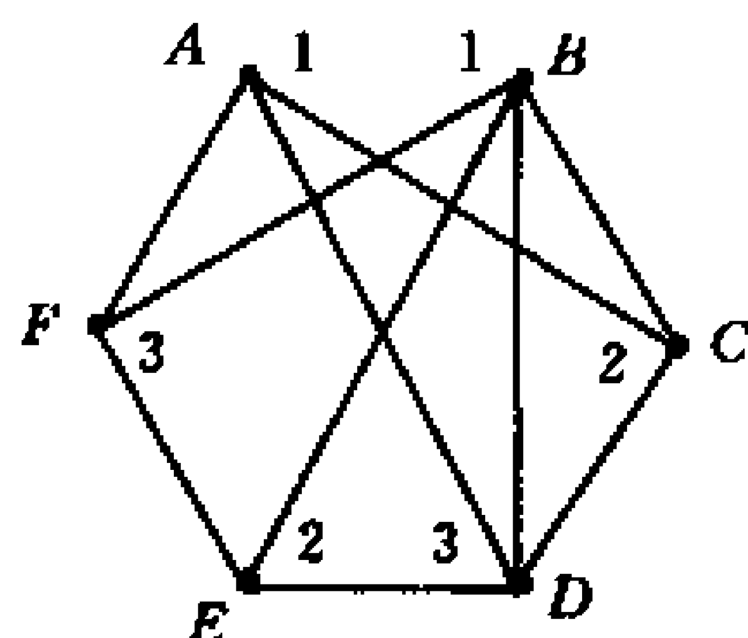


图 4.25

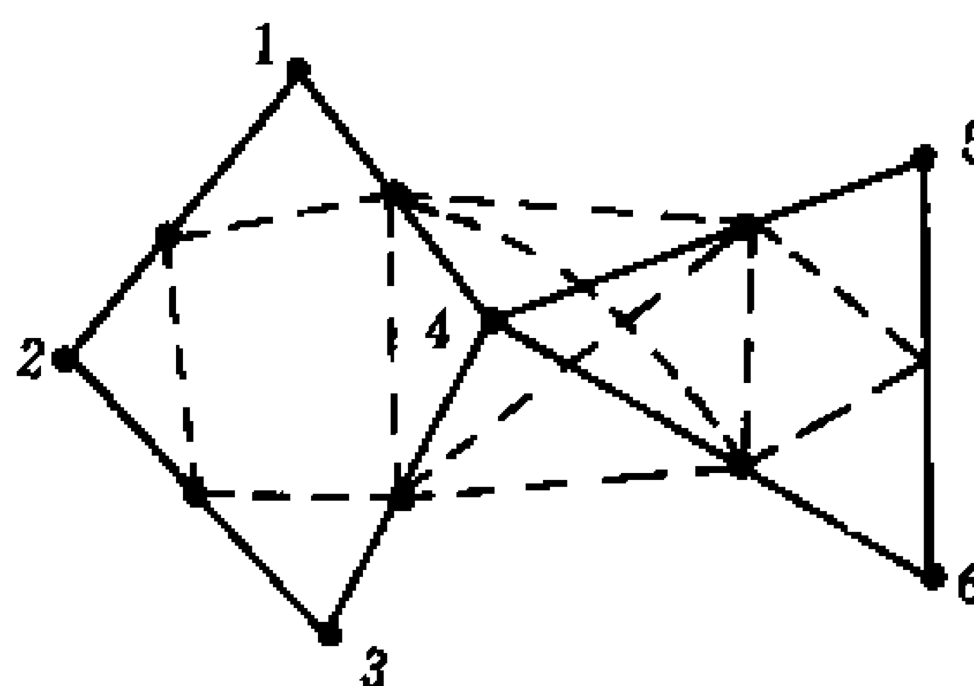


图 4.26

G 的边着色问题可以通过下述方法转化为对 G' 的结点着色。在 G 的每条边 e_i 上设置一个结点 v'_i，如果 e_i 与 e_j 关联于同一结点 v_k，则 G' 中有边(v'_i, v'_j)。比如图 4.26 的 G' 如虚线边所示。这样 G 的边着色就等价于 G' 的结点着色。因此以下仅讨论 G 的结点着色问题。

结点着色问题只需要针对简单图。某些熟悉的图的色数比较容易决定。

1. 若 G 是空图，则 $\gamma(G)=1$。

2. 若 G 是 n 个结点的完全图，则 $\gamma(G)=n$。

3. $G=K_n-e$，$\gamma(G)=n-1$。

4. G 是二分图，$\gamma(G)=2$。

5. G 是 $2n$ 个结点的回路，$\gamma(G)=2$。

6. G 是 $2n+1$ 个结点的回路，$\gamma(G)=3$。

7. G 是 $n(\geqslant 2)$ 个结点的树，$\gamma(G)=2$。

定理 4.6.1 一个非空图 G，$\gamma(G)=2$ 当且仅当它没有奇回路。

证明：充分性。在 G 中确定一个林 T'，其每个连通子图都是树 T，$\gamma(T)=2$。由于每个回路都是偶回路。所以加入每一条余树边都不会使结点着色发生变化，因此 $\gamma(G)=2$。必要性。如果 G 中有奇回路，则 $\gamma(G)\geqslant 3$，矛盾。

利用此定理，立即得知二分图中的回路都是偶回路。

例 4.6.2 平面连通图 G 的域可 2 着色当且仅当 G 中存在欧拉回路。

证明：G 存在对偶图 G^*，原命题变为 G^* 点 2 着色当且仅当连通图 G 有欧拉回路。先证必要性，由定理 4.6.1，G^* 每个回路都是偶回路，即它的每个域的边界都是偶数。由于 $(G^*)^*=G$，G^* 的每个域 f_i 内都有 G 的一个结点 v_i，由 D 过程知，$d(v_i)$是偶数。故 G 有欧拉回路。充分性。由于 G 中每个结点的度都是偶数，因此 G^* 中包围每个结点 v_i 的回路都是偶回路，且任意两个偶回路的对称差依然是偶回路。所以 G^* 中没有奇回路，$\gamma(G^*)=2$。

定理 4.6.2 对于任意一个图 G。

$$\gamma(G) \leqslant d_0 + 1。$$

其中 $d_0 = \max d(v_i)$。

证明：对 G 的结点进行归纳，$n=1$ 时成立。设 $n=k-1$ 时成立，当 $n=k$ 时，从 G 中任意移去一点 v_i 得 G'，$V(G')=k-1$。于是 $\gamma(G') \leqslant d_0'+1$，其中 d_0' 是 G' 的结点最大度，由于 $d_0' \leqslant d_0$，因此 $\gamma(G') \leqslant d_0+1$。即 d_0+1 种颜色可以对 G' 的结点着色，放回结点 v_i 恢复成 G，由于 $d(v_i) \leqslant d_0$，所以必有一种与 v_i 的邻点都不相同的颜色可对 v_i 着色。

这个定理还可以进一步改进。

定理 4.6.3 对于任意一个图 G。

$$\gamma(G) \leqslant 1 + \max\delta(G')。$$

其中 $\delta(G')$ 是 G 的导出子图 G' 中结点的最小度，极大是对所有的 G' 而言。

证明：当 G 为空时显然正确。设 $\gamma(G)=k \geqslant 2$，令 H 是满足 $\gamma(H)=k$ 的任何一个 G 的最小导出子图，于是 H 对它的所有结点 v 来说，有 $\gamma(H-v)=k-1$。所以在 H 中结点 v 至少有 $k-1$ 个邻接点，即 $d(v) \geqslant k-1$，于是 $\delta(H) \geqslant k-1$。而对于 H 的所有导出子图 $\{H'\}$，必有 $\delta(H) \leqslant \max\delta(H')$；同时 H' 也是 G 的某个导出子图。对于 G 的全部导出子图 $\{G'\}$，又有 $\max\delta(H') \leqslant \max\delta(G')$。由上述不等式即得

$$\gamma(G) = k \leqslant 1 + \max\delta(G')。$$

具体给定一个图 G，又怎样确定它的色数呢？下面我们介绍色数的一种求解方法。

定义 4.6.3 设 i,j 是简单图 G 不相邻的两个结点。令 $G_{ij}=G+e_{ij}$，$\mathring{G}_{ij}$ 也是一个简单图，其结点集 $\mathring{V} = V-\{i,j\}+\{ij\}$，边集

$$\mathring{E} = E - \{(k,i) \mid (k,i) \in E\} - \{(k,j) \mid (k,j) \in E\} + \{(k,ij) \mid (k,i) \in E \text{ 或 } (k,j) \in E\}。$$

例 4.6.3 设结点 i 和 j 如图 4.27(a)所示，(b)是 $\overline{G}_{ij}$，(c)是 $\mathring{G}_{ij}$。

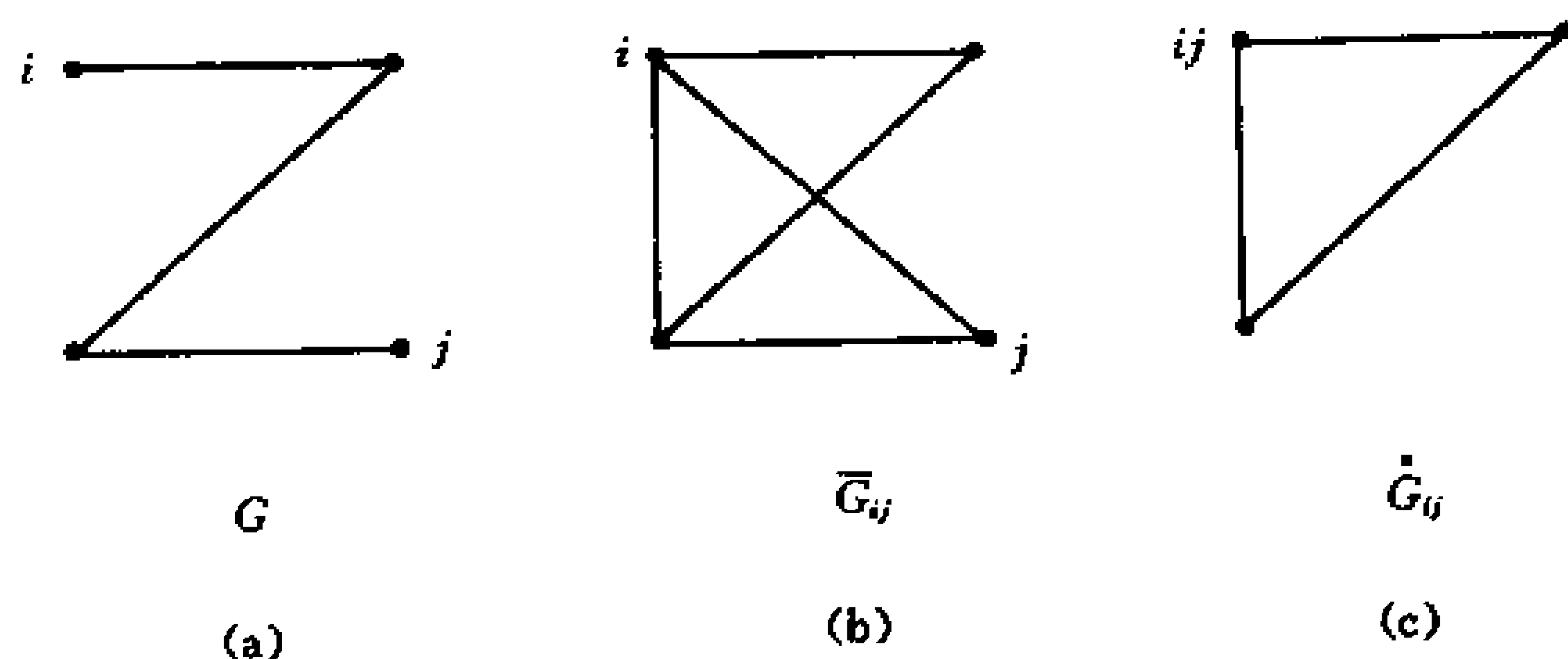


图 4.27

定理 4.6.4 设 i,j 是简单图 G 不相邻的结点，则

$$\gamma(G) = \min\{\gamma(\overline{G}_{ij}), \gamma(\mathring{G}_{ij})\}。$$

证明：对 G 中结点的任何着色，i 和 j 或者将着以同色，或者异色，二者必居其一。设 i,j 着以异色情况下的 G 的最少着色数为 $\gamma(G(i,j\text{ 异色}))$，i,j 着以同色情况下的最少着

色数是$\gamma(G(i,j$同色$))$. 这样，

$$\gamma(G)=\min\{\gamma(G(i,j\text{异色})),\gamma(G(i,j\text{同色}))\}。$$

显然式中

$$\gamma(G(i,j\text{异色}))=\gamma(\overline{G}_{ij})。$$

$$\gamma(G(i,j\text{同色}))=\gamma(\mathring{G}_{ij})。$$

因此定理得证。

根据这个定理我们可以递推计算$\gamma(G)$。

例 4.6.4 图 4.28 给出了G的色数$\gamma(G)$的计算过程：

∵ $$\gamma(\overline{G}_{ij})=4,\gamma(\mathring{G}_{ij})=3,$$

∴ $$\gamma(G)=3.$$

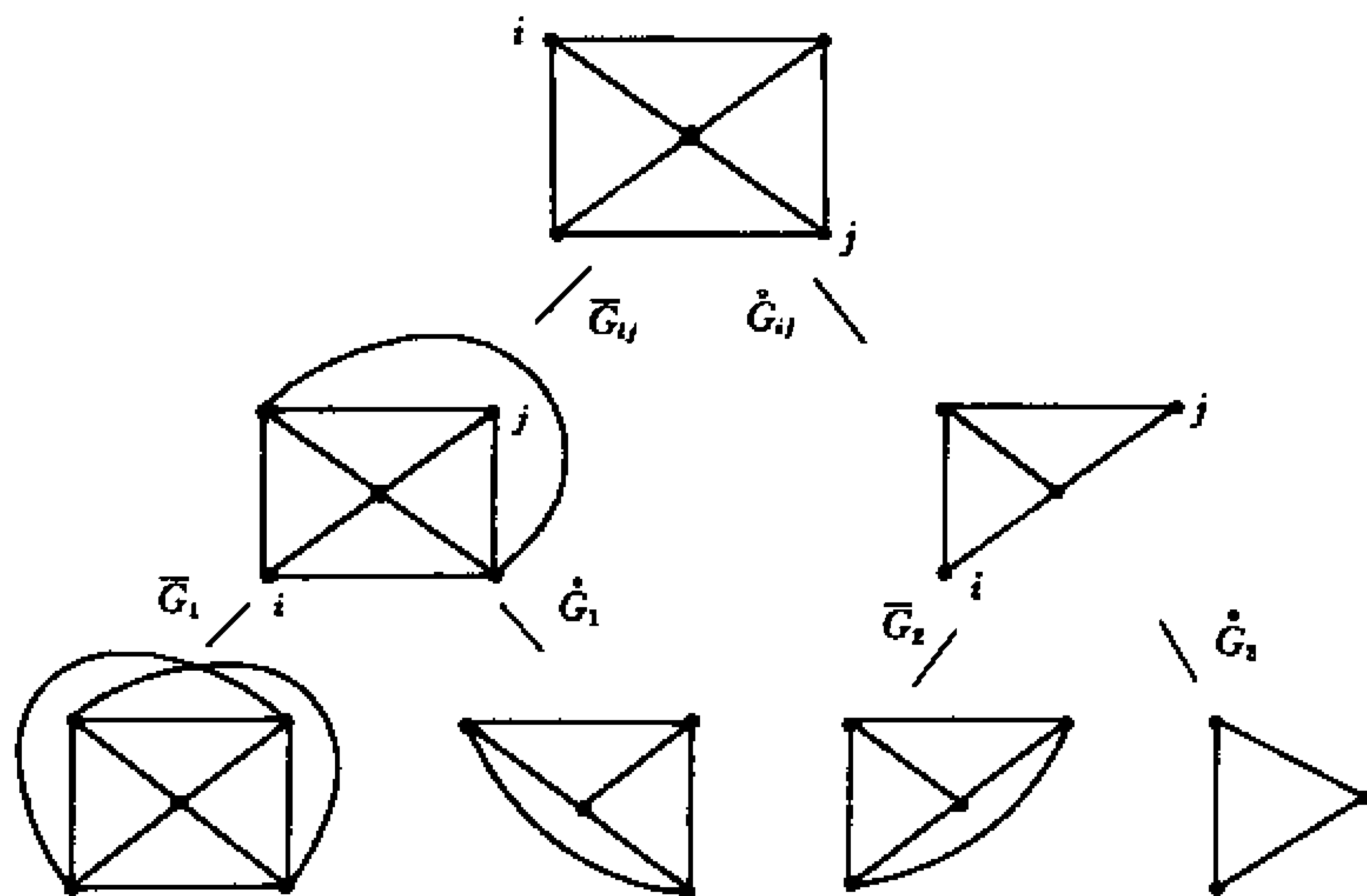


图 4.28

给定一个图G,如果最多使用t种颜色对它的结点进行着色,满足相邻结点着以不同颜色,那么会有多少种不同的方案呢?

我们用$f(G,t)$表示这种不同的结点着色数目。当然,若$t<\gamma(G)$,$f(G,t)=0$。实际上,满足$f(G,t)>0$的最小t值就是G的色数。这样,五色定理可以表述成:对于每一个可平面图,$f(G,5)>0$。而四色猜想则是:$f(G,4)>0$。

例如,对K_3来说有t种方法可对其第一个结点着色,而第 2 个结点只有$t-1$种方法,第 3 个结点有$t-2$种。因此$f(K_3,t)=t(t-1)(t-2)$。

一般说来,令m_i是i种颜色对G的结点着色的方案数。那么用t种颜色对G着色,恰好用上了i种的全部着色方案是$m_iC(t,i)$,这样我们有

$$f(G,t)=m_1C(t,1)+m_2C(t,2)+\cdots+m_nC(t,n)$$

$$=m_1t+\frac{1}{2!}m_2t(t-1)+\cdots+\frac{1}{n!}m_nt(t-1)\cdots(t-n+1)。$$

这就是图G的一个最简单的色数多项式,它是t的一个n次多项式。

定理 4.6.5 $f(K_n,t)=t(t-1)\cdots(t-n+1)$。

当 $t<n$ 时，$f(K_n,t)=0$，而 $t=n$ 时，$f(K_n,t)=n!$。

定理 4.6.6 $f(T_n,t)=t(t-1)^{n-1}$。

这由 $\gamma(T_n)=2$ 即可得证。当 $t=2$ 时，$f(T_n,t)=2$。

对于一般的图 G，我们可以通过下述方法计算其色数多项式。

定理 4.6.7 设 i,j 是 G 的不相邻结点，则

$$f(G,t) = f(\overline{G}_{ij},t) + f(\mathring{G}_{ij},t)。$$

其中 $\overline{G}_{ij}$，$\mathring{G}_{ij}$ 由定义 4.6.3 给出。

证明：用 t 种颜色对 G 着色的全部 $f(G,t)$ 种方案中，对结点 i 和 j 的着色只有二类：i 与 j 着以异色，这类的总数目即是 $f(\overline{G}_{ij},t)$；否则 i 与 j 必着以同色，而这类的总数是 $f(\mathring{G}_{ij},t)$，因此定理得证。

例 4.6.5 图 4.28 G 的色数多项式是

$$\begin{aligned}f(G,t) &= f(K_5,t) + 2f(K_4,t) + f(K_3,t)\\&= t(t-1)(t-2)(t-3)(t-4) + 2t(t-1)(t-2)(t-3)\\&\quad + t(t-1)(t-2)\\&= t(t-1)(t-2)(t^2-5t+7)\end{aligned}$$

如果至多用 3 种颜色，那么 $f(G,3)=6$。

例 4.6.6 求 n 个结点回路 C_n 的色数多项式。

解：设 G 是 n 个结点的一条路，i 和 j 是它的两个端点，则 $\overline{G}_{ij}$ 就是 n 个结点的回路 C_n，$\mathring{G}_{ij}$ 是 $n-1$ 个结点的回路 C_{n-1}。如图 4.29 所示，由定理 4.6.7，

$$f(C_n,t) = f(T_n,t) - f(C_{n-1},t),$$

即：

$$f(C_n,t) + f(C_{n-1},t) = t(t-1)^{n-1}。$$

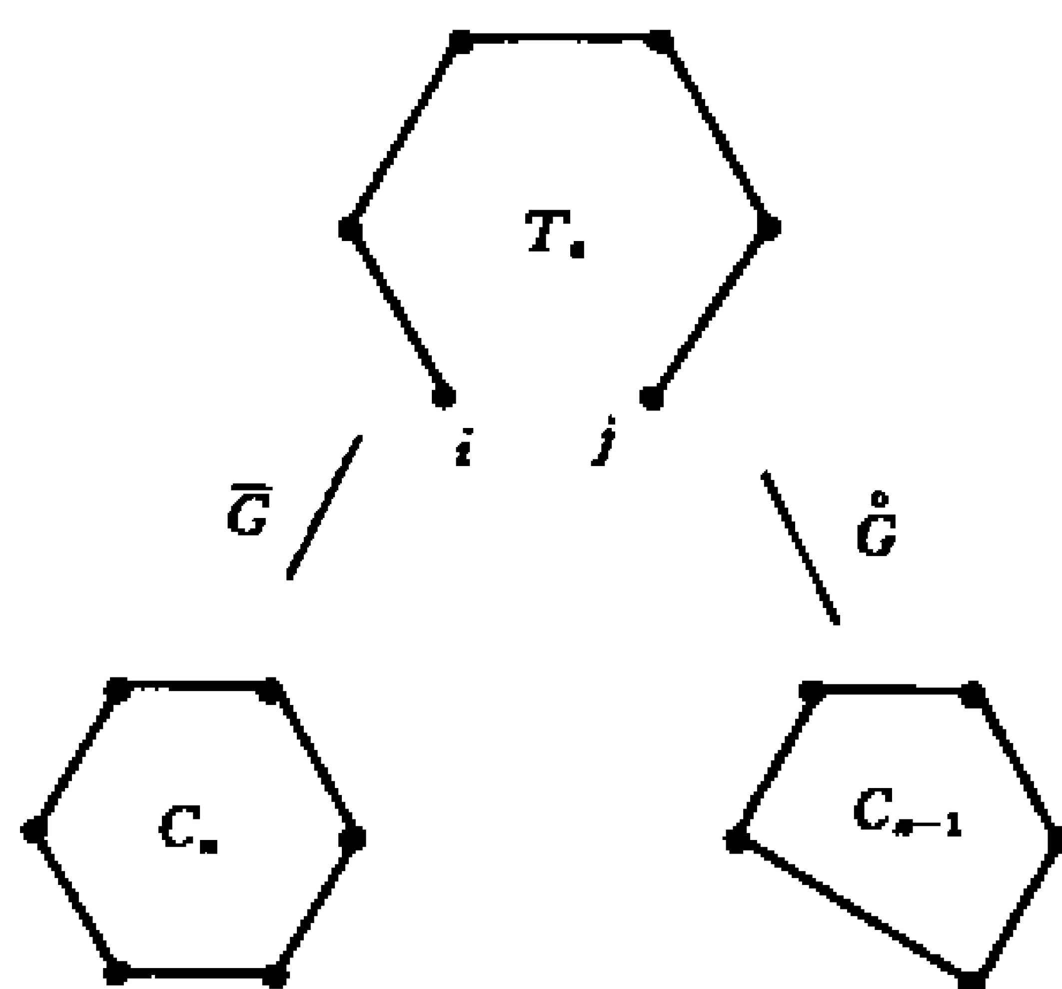


图 4.29

利用此递推公式可得

$$f(C_n,t) = (t-1)^n + (-1)^n(t-1)。$$

习 题 四

1. 设简单平面图的域的数目 $d<12$，每点的度 $d(v_i)\geqslant 3$，证明至少有一个域的边界数小于 5。

2. 证明：在 $n\geqslant 4$ 的极大平面图中，每个结点的度都大于等于 3。

3. 设 G 是结点数大于 10 的简单图，证明 G 和 $\overline{G}$ 至少有一个是非平面图。

4. 证明：

1）结点数 $n<12$ 的平面图可以点 4 着色。

2）结点数 $n<12$ 的平面图可以域 4 着色。

5. 求所有的正凸多面体。

6. 设 G 是无割边的平面图，且每两个面之间最多有一条公共边，证明：

1）G 中至少有两个面有相同的边界数。

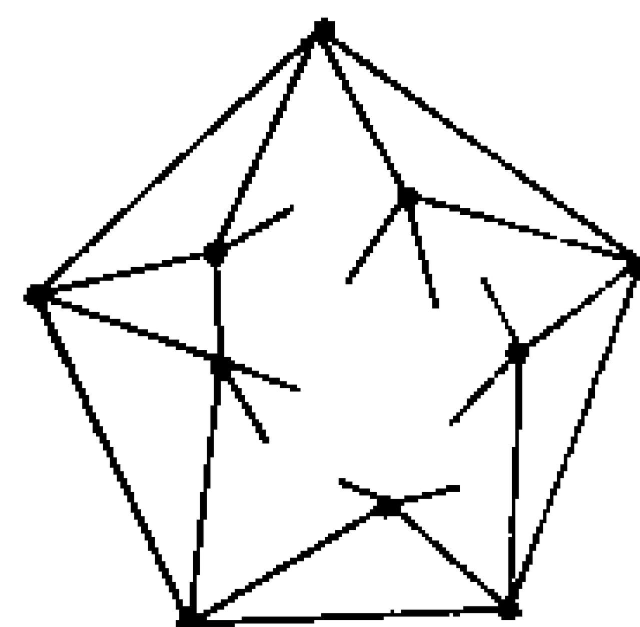
2）若各面最小的边界数是 5，则 G 中至少有 12 个这样的面。

7. 试证：不存在这样的平面图，它有 5 个域，且任意两个域之间至少有一条公共边界。

8. 设简单平面图 G 的结点数 $n\geqslant 4$，证明 G 中至少有 4 个结点的度不大于 5。

9. 证明：若无割边的平面图除一个域外，其余各域的边界数都可以被整数 $d(>1)$ 整除，则 G 的域不能 2 着色。

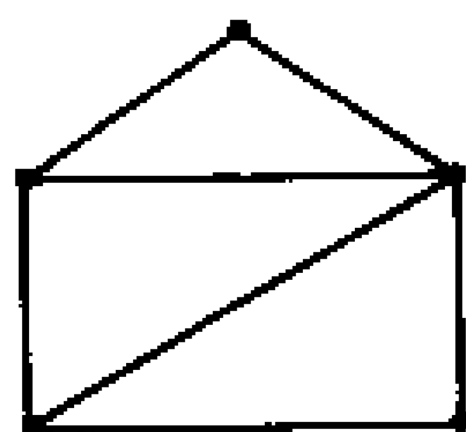
10. 你能在五边形 $ABCDE$（如图）内部画出有限个三角形，保证每个结点的度是偶数吗？试说明理由。



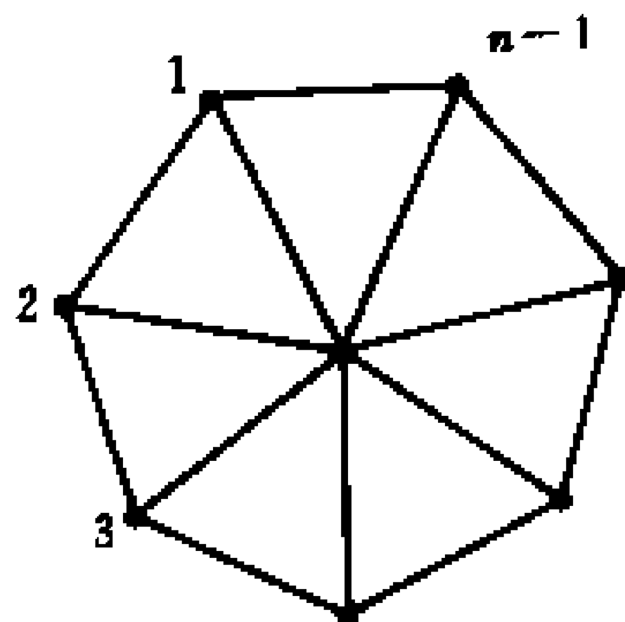
题图 4.10

11. 设简单连通图 G 的结点数是 15，其中 8 个点的度是 4，6 个点的度是 6，一个点的度是 8，证明 G 是非平面图。

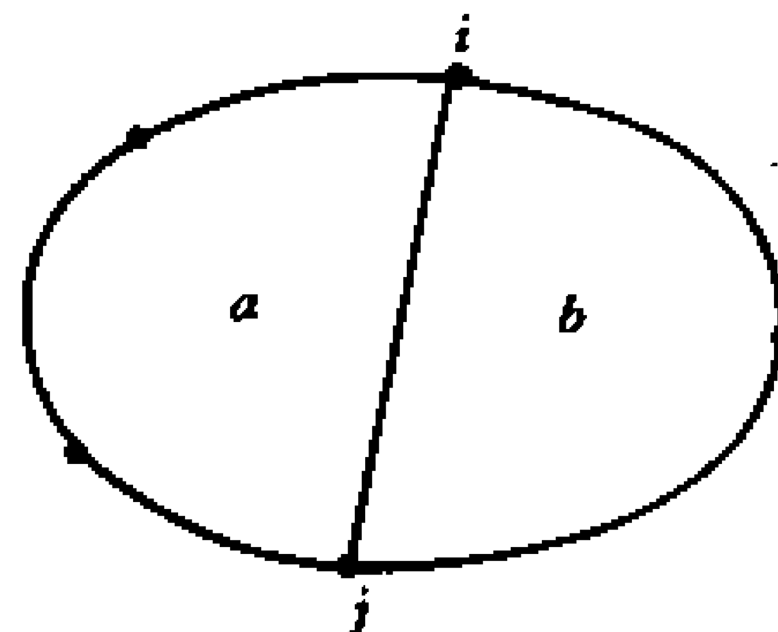
12. 设 G 是每个面都是三角形的平面图，现用 3 种颜色对它的所有结点任意着色。证明：顶点上恰好得到了这 3 种颜色的面的数目是偶数个。



题图 4.13



题图 4.14



题图 4.16

13. 求题 4.13 图的色数与色数多项式。

14. 求 n 个结点轮形图 W_n 的色数与色数多项式。

15. 完成例 4.6.6 的计算。

16. 设 G 如题 4.16 图所示，其中 a 是含 m 个结点的初级回路，b 是含 n 个结点的初级回路，(i,j) 是它们的公共边，求 G 的色数与色数多项式。

17. 编写 DMP 算法的程序，并验证 K_5-e 和 $K_{3,3}$ 的平面性。

第五章　匹配与网络流

5.1　二分图的最大匹配

图的匹配问题有其丰富的实际背景，它涉及了二分图与一般图的最大匹配，二分图与一般图的最佳匹配等，除了一般图的最佳匹配之外，本章都将一一进行讨论

例 5.1.1　m 项工作准备分配给 n 个人去做，如图 5.1 所示，其中边 (x_i, y_j) 表示 x_i 可以从事 y_j，如果每个人最多从事其中一项，且每项工作只能由一人承担。问怎样才能让尽可能多的人安排上任务。

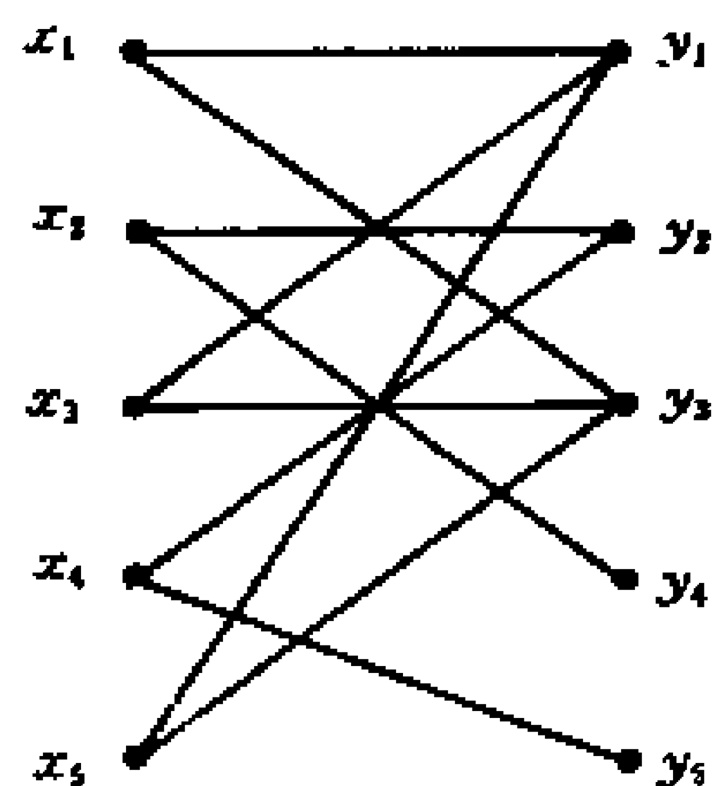
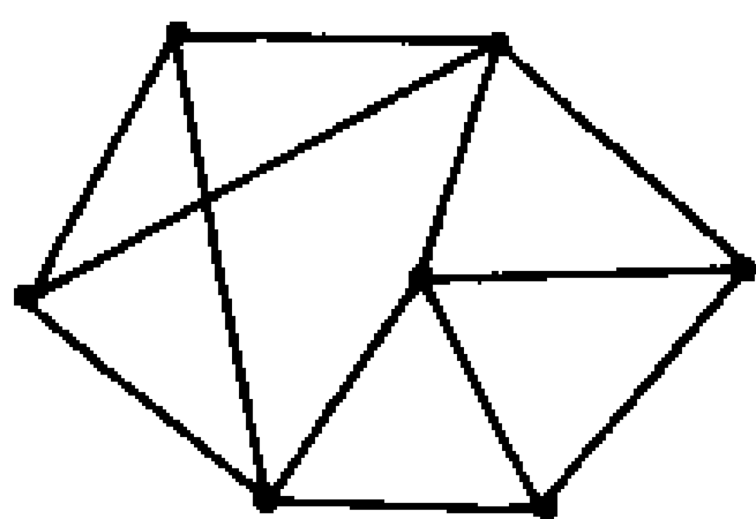


图 5.1

图 5.1 是二分图，按照要求，如果 x_i 从事了 y_j，就不允许再从事 y_k，同时 y_j 也不再允许其他人承担。因此，它相当于用一种颜色，比如红色对 G 的边进行着色，保证每个结点最多只与一条红色边关联。这种红色边的集合记为 M，它就称为匹配。原问题就是计算 G 中包含边数最多的一个匹配 M。

例 5.1.2　二次大战期间，盟军许多飞行人员到英国参加对法西斯德国的空袭行动，当时每架飞机需要领航员和飞行员各 1 人。其中有些人只能领航，一些人只会驾驶，也有人两者均会。加之二人语言要求相通，因此如果以结点表示人，边表示两者语言相通并且一人可领航另一人可驾驶。就会得到如 5.2 所示的图，这是一个简单图 G。那么最多的编队方案就是计算 G 中的一个最大匹配。


图 5.2

定义 5.1.1　令 M 是图 G 的边子集，若 M 中任意两条边都没有共同的结点，则称 M 是 G 的一个匹配，其中与 M 的边关联的结点称为饱和点，否则称为非饱和点。

定义 5.1.2　设 M 是 $G=(V,E)$ 中的一个匹配，如果对 G 的任意匹配 M'，都有 $|M| \geqslant |M'|$，就说 M 是 G 的一个最大匹配。

定义 5.1.3　给定了 G 的一个匹配 M，G 中属于 M 与不属于 M 的边交替出现的道路称为交互道路。

有时这种交互道路可能构成回路。

定义 5.1.4　设 P 是 G 中关于匹配 M 的一条交互道路，如果 P 的两个端点是关于 M 的非饱和点，那么它就称为可增广道路。

可增广道路 P 一定包含奇数条边，且其中不属于匹配 M 的边比 M 中的边多一条。同时 $P \oplus M$ 仍然是 G 的一个匹配 M'，它使 P 的两个端点变成饱和点，这时 $|M'| = |M| + 1$，即 M' 是比 M 更大的匹配。

定理 5.1.1 M 是 G 的最大匹配当且仅当 G 中不存在关于 M 的可增广道路。

证明：必要性。若存在 M 的可增广道路 P，则 $M \oplus P = M'$ 是 G 的一个新匹配，且 $|M'|>|M|$，与 M 是最大匹配矛盾。充分性。如果匹配 M 不是 G 的最大匹配，则存在一个最大匹配 M'，作 $G'=M' \oplus M$，我们逐一分析 G' 中三种可能的连通支：

1. 孤立结点，当 $(v_i, v_j) \in M' \cap M$ 时会出现孤立点 v_i，v_j。

2. 交互回路，该回路中属于 M' 和属于 M 的边数相同。

3. 交互道路。如果不存在增广道路，那么 $|M'|=|M|$，与假设矛盾。如果存在 M 关于 M' 的增广路，又与 M' 是最大匹配矛盾。由于 $|M'|>|M|$，故必定存在 M' 关于 M 的可增广交互道，即 G 中存在关于 M 的可增广道路。

定理 5.1.1 是二分图和一般图最大匹配算法的依据。不过由于二分图的所有回路都是偶回路的特点，因此它的最大匹配算法较为简单，而一般图的最大匹配问题将在 5.4 节中进行讨论。

计算二分图最大匹配的一个好算法是匈牙利算法。描述如下：

匈牙利算法

（输入为二分图 $G=(X, Y, E)$；结点标记 0：表示尚未搜索，1：表示是饱和点，2：表示是无法扩大匹配的结点）。

1. 任给一初始匹配 M，给饱和点"1"标记

2. 判 X 中的各结点是否都已有非零标记

    2.1 是。M 是最大匹配，结束

    2.2 否。找一"0"标记点 $x_0 \in X$，

    令 $U \leftarrow \{x_0\}$，$V \leftarrow \Phi$。

3. 判集合 U 的邻接点集 $\Gamma(U)=V$?

    3.1 是，x_0 无法扩大匹配，给 x_0 标记"2"，转 2。

    3.2 否，在 $\Gamma(U)-V$ 中找一点 y_i，判 y_i 是否标"1"。

        3.2.1 是，则有边 $(y_i, z) \in M$。令

        $U \leftarrow U \cup \{z\}, V \leftarrow V \cup \{y_i\}$，转 3。

        3.2.2 否，存在从 x_0 至 y_i 的可增广路 P，

        令 $M \leftarrow M \oplus P$，给 x_0，y_i 标记 1，转 2。

例 5.1.3 图 5.3 中，设初始匹配 $M=\{(x_1, y_1), (x_3, y_4), (x_4, y_5)\}$。用匈牙利算法求其最大匹配的过程如下：

（1）$U=\{x_2\}, V=\Phi$。

$\Gamma(U)=\{y_1, y_6\}, y_6 \in \Gamma(U)-V$，且无标记，

$\therefore$ 增广路 $P=(x_2, y_6)$。

$M=\{(x_1, y_1), (x_3, y_4), (x_4, y_5), (x_2, y_6)\}$。

（2）$U=\{x_5\}, V=\Phi$。

$\Gamma(U)=\{y_5, y_6\}, y_5 \in \Gamma(U)-V$。

$U=\{x_5, x_4\}, V=\{y_5\}$。

$\Gamma(U)=\{y_5, y_6\}, y_6 \in \Gamma(U)-V$。

$U=\{x_5,x_4,x_2\},V=\{y_5,y_6\}$。

$\Gamma(U)=\{y_5,y_6,y_4\},y_4\in\Gamma(U)-V$。

$U=\{x_5,x_4,x_2,x_3\},V=\{y_5,y_6,y_4\}$。

$\Gamma(U)=\{y_5,y_6,y_4,y_2\},y_2\in\Gamma(U)-V$ 且无标记。

∴ 有增广路 $P=(x_5,y_6,x_2,y_4,x_3,y_2)$。

$M=\{(x_1,y_1),(x_4,y_5),(x_5,y_6)(x_2,y_4),(x_2,y_3)\}$。

(3)$U=\{x_6\},V=\Phi$。

$\Gamma(U)=\{y_6\},y_6\in\Gamma(U)-V$。

$U=\{x_6,x_5\},V=\{y_6\}$。

$\Gamma(U)=\{y_6,y_5\},y_5\in\Gamma(U)-V$。

$U=\{x_6,x_5,x_4\},V=\{y_6,y_5\}$。

$\Gamma(U)=\{y_6,y_5\},\Gamma(U)=V$。给 x_6 标记 2。结束。

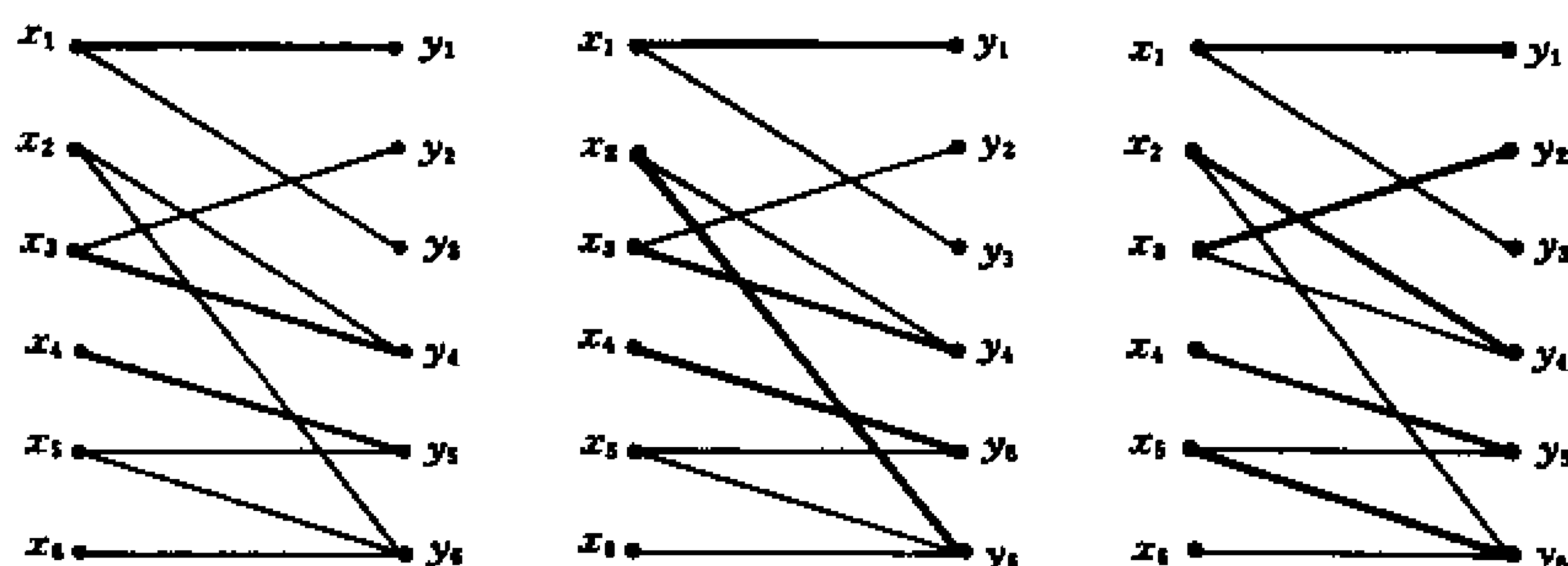


图 5.3

因此，其最大匹配是 $M=\{(x_1,y_1),(x_4,y_5),(x_5,y_6),(x_2,y_4),(x_3,y_2)\}$。

定理 5.1.2 最大匹配匈牙利算法的计算复杂性是 $O(mn)$，其中 n 是二分图 G 中 X 的结点数。

证明：初始匹配可以是空匹配，算法最多找 n 条增广路，每找一条增广路时，最多判断 m 条边，因此其计算复杂性是 $O(mn)$。

5.2 完全匹配

二分图 $G=(X,Y,E)$ 的最大匹配 M 包含的边数不会超过 $|X|$，若 $|M|=|X|$，则称 M 是完全匹配。特别地，如果 $|M|=|X|=|Y|$，则称 M 是完美匹配。直观地看，如果每个结点 x 关联的边愈多，则最大匹配的边数可能愈大。例如图 5.4(a)有完全匹配，而(b)没有完全匹配。那么满足什么条件 G 中就会有完全匹配呢？霍尔(Hall)定理给出了判别的标准。

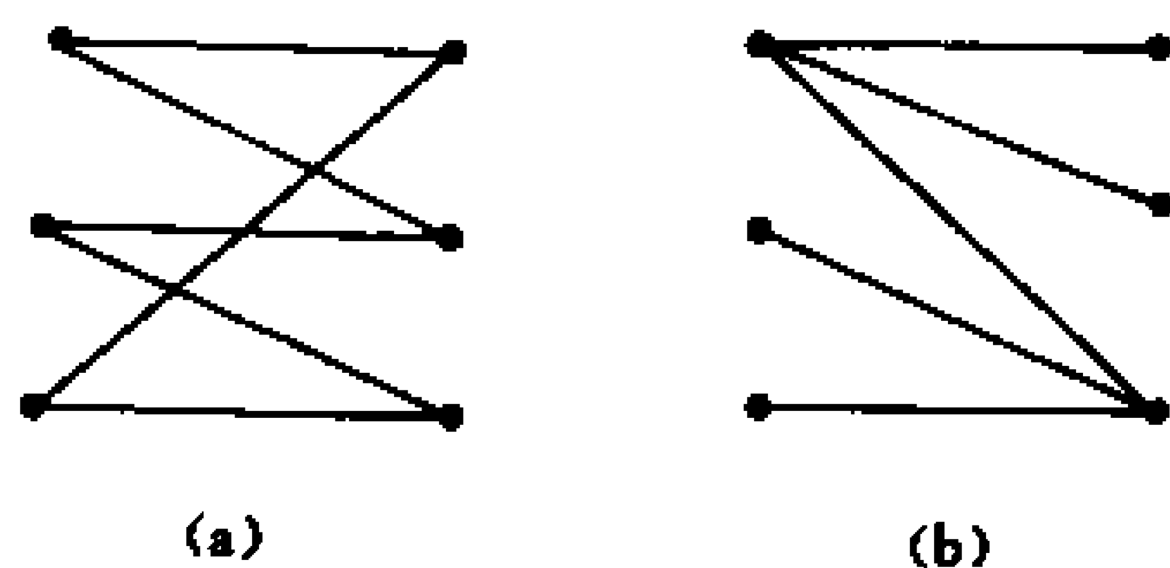


图 5.4

定理 5.2.1 在二分图 $G=(X,Y,E)$ 中，

X 到 Y 存在完全匹配的充要条件是对于 X 的任意子集 A，恒有

$$|\Gamma(A)| \geq |A|。$$

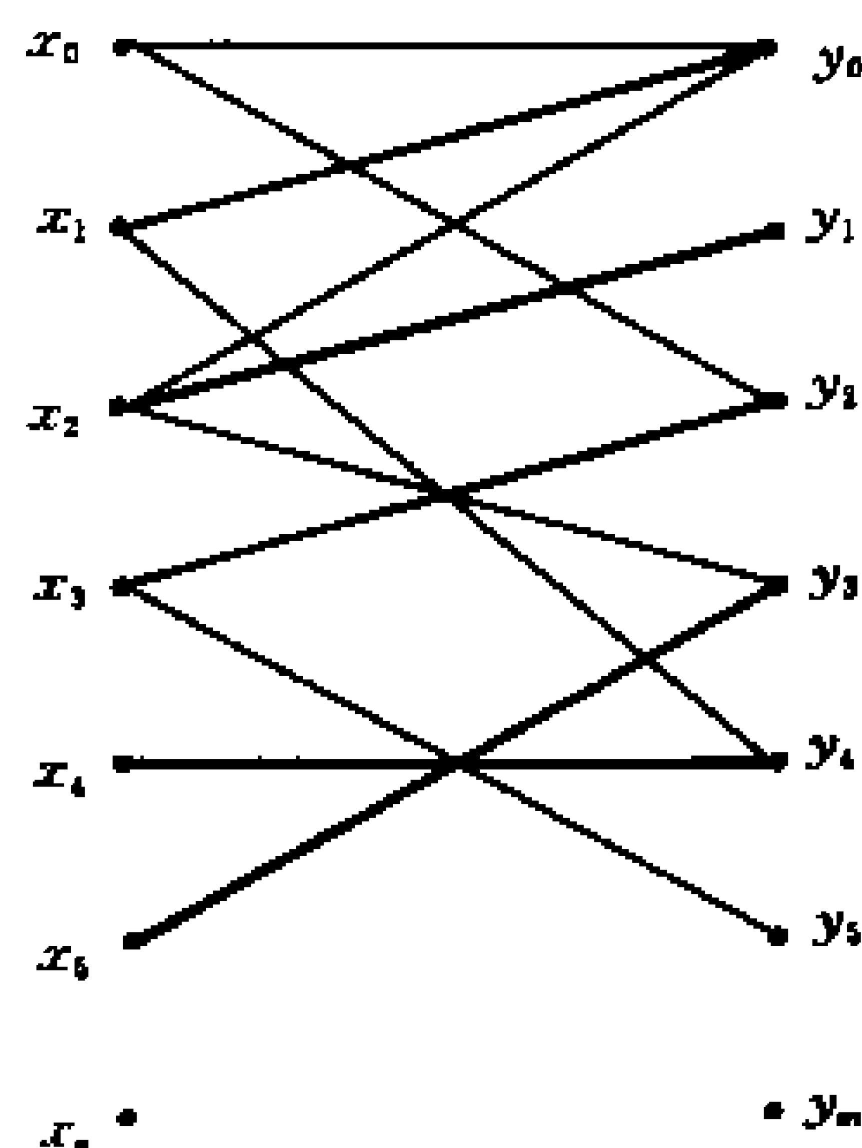


图 5.5

证明：必要性。若存在子集 $A\subseteq X$，使 $|A|>|\Gamma(A)|$。则 A 中的结点无法全部匹配，因此 X 到 Y 不可能有完全匹配。充分性。假定 G 的一个最大匹配 M 不是完全匹配，一定存在结点 $x_0\in X$ 是关于 M 的非饱和点。如果 $\Gamma(x_0)=\Phi$，则令 $A=\{x_0\}$，于是 $|\Gamma(A)|<|A|$，不满足条件。如果 $\Gamma(x_0)\neq\Phi$，对某一个 $y_j\in\Gamma(x_0)$，若 y_j 关于 M 为非饱和点，则存在增广路 (x_0,y_j)，与 M 是最大匹配矛盾。因此 $y_j\in\Gamma(x_0)$ 都是关于 M 的饱和点。这样可以寻找以 x_0 为端点的相对于 M 的一切交互道，记交互道中结点 y_j 的集合为 Y_1，结点 x_i 的集合为 X_1，根据匹配的性质 Y_1 的结点与 X_1-x_0 的结点之间存在一一对应，于是 $|X_1|>|Y_1|$，即 $|X_1|>|\Gamma(X_1)|$。

推论 5.2.1 若二分图 $G=(X,Y,E)$ 的每个结点 $x_i\in X$，都有 $d(x_i)\geq k$，每个结点 $y_j\in Y$，都有 $d(y_j)\leq k$，那么 X 到 Y 存在完全匹配。

证明：对任意子集 $A\subseteq X$，设它的结点总共与 m 条边关联，于是有 $m\geq k|A|$，这 m 条边又与 Y 中的 $|\Gamma(A)|$ 个结点相关联，又有 $m\leq k|\Gamma(A)|$，因此 $|\Gamma(A)|\geq|A|$，由定理 5.2.1 即得。

例 5.2.1 在一个舞会上男女各占一半，假定每位男士都认识 k 位女士，每位女士也认识 k 位男士。那么一定可以安排得当，使每位都有认识的人作为舞伴。

证明：用结点 x_i 表示每位男士，y_j 表示每位女士，互相认识者用边连之。于是得到二分图 $G=(X,Y,E)$，图中每个结点 x_i 有 $d(x_i)=k$，y_j 有 $d(y_j)=k$。满足 $d(x_i)\geq k$，$d(y_j)\leq k$，由推论 5.2.1，X 到 Y 有完美匹配 M。M 就是一种安排方案。

二分图的完全匹配一定是最大匹配，而最大匹配不一定就是完全匹配，那么它们之间有什么内在联系呢？

定理 5.2.2 在二分图 $G=(X,Y,E)$ 中，X 到 Y 最大匹配的边数是 $|X|-\delta(G)$，其中 $\delta(G)=\max\limits_{A\subseteq X}\delta(A)$，$\delta(A)=|A|-|\Gamma(A)|$，$\delta(A)\geq 0$。

证明略。

例 5.2.2 10 个人有 10 件不同的乐器，其中 3 人只会拉小提琴，其余 7 人每件乐器都会，若每人只用一件乐器，则由定理 5.2.2，最多只有 8 人能同时登台演出。

二分图是一个图，当然可以用邻接矩阵表示。由于其全部的边都跨越在 X 和 Y 之间，因此我们可以将邻接矩阵进行简化，成为 $|X|\times|Y|$ 的一个矩阵。比如图 5.6 的邻接矩阵是

$$A=\begin{bmatrix}0&0&0&1&0\\0&1&0&0&0\\0&1&0&0&0\\1&1&0&0&1\\0&0&0&1&0\\0&0&1&0&1\end{bmatrix}$$

这样 G 中的最大匹配数 r 就是 A 中不在同行同列非零元的最多个数。如果矩阵 A 是 $p\times q$ 的，显然有 $r\leqslant\min(p,q)$。

另外我们也可以适当地选取 A 的某些行和列，使这些行和列能盖住 A 中的全部非零元，这称之为 A 的覆盖，当然如果盖住 A 的全部 p 行，或全部 q 列，就一定会盖住所有非零元，但这不一定是最少选取的行与列，比如图 5.6 的矩阵 A，如果盖住其第 4、6 行，第 2、4 列，就可以覆盖其全部非零元。因此在矩阵 A 的全部覆盖中，一定存在最小覆盖，其覆盖数为 s，显然 $s\leqslant\min(p,q)$。

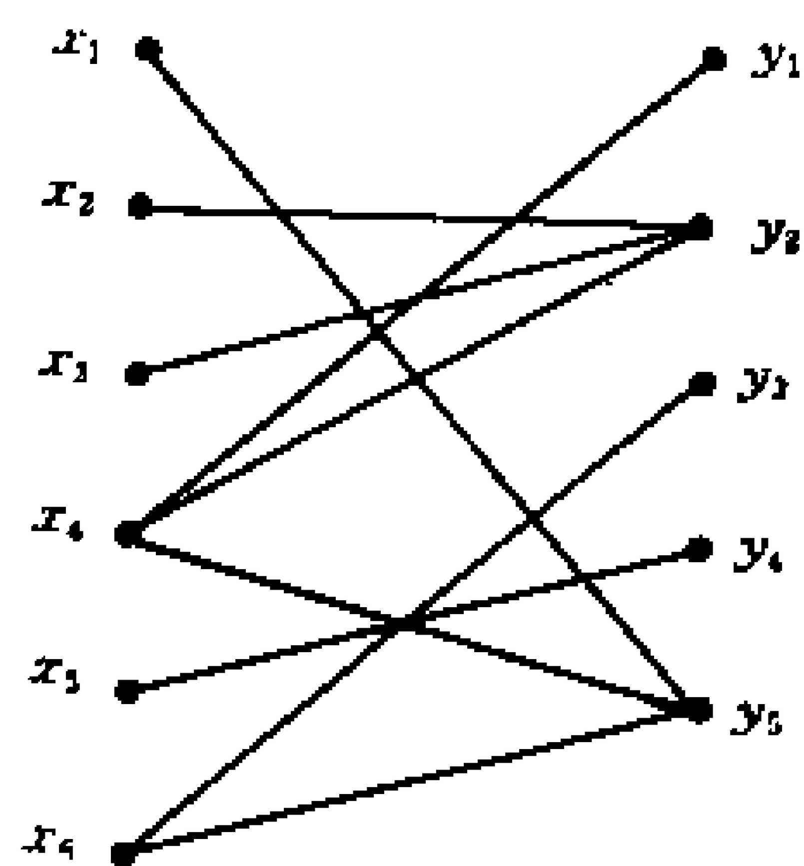


图 5.6

定理 5.2.3 设 r 是二分图 G 的最大匹配数，s 是其邻接矩阵的最小覆盖数，则有 $r=s$。

证明：因为每个不在同行同列的非零元需要一行或一列才能盖住，所以 r 个不在同行同列的非零元需要 r 行、列才能盖住，而 s 个不同的行、列盖住了矩阵 A 的全部非零元，自然也盖住了 r 个不在同行同列的非零元。因此 $s\geqslant r$。再证 $r\geqslant s$。不失一般性，设最小覆盖盖住了 A 的 c 行、d 列，即 $s=c+d$。设这 c 行对应的结点子集是 X_c，其余为 $X-X_c$；d 列对应的结点集是 Y_d，其余为 $Y-Y_d$。把矩阵 A 的行、列进行调整，如图 5.7 所示，显然 A_{11} 每行都被覆盖，A_{22} 每列都被覆盖，A_{12} 中每个元素既被行也被列所覆盖，而 $A_{21}=0$。

	$Y-Y_d$	Y_d
X_c	A_{11}	A_{12}
$X-X_c$	A_{21}	A_{22}

图 5.7

现证明 X_c 到 $Y-Y_d$ 存在完全匹配。在 A_{11} 中任取 $|V'|$ 行，这些行中的非零元至少分布在它的 $|V'|$ 个不同列上。否则，不覆盖这 $|V'|$ 行，而覆盖这些更少的列，A 中的所有非零元仍然全部覆盖，这时所用的覆盖数比原先要少，与原来是最小覆盖矛盾。这就是说，对 X_c 的任意子集 V'，它在 $Y-Y_d$ 中的邻接点集是 $\Gamma(V')$，总有 $|\Gamma(V')|\geqslant|V'|$。根据定理 5.2.1，$X_c$ 到 $Y-Y_d$ 存在完全匹配 M_1，$|M_1|=c$。同理 Y_d 到 $X-X_c$ 也存在完全匹配 M_2，$|M_2|=d$，$M_1\cup M_2$ 仍然是 G 的一个匹配，$|M_1\cup M_2|=c+d=s$。因此 G 的最大匹配数 $r\geqslant s$。

定理 5.2.3 不但揭示了匹配与覆盖之间的关系，而且也是最佳匹配算法的基本依据之一。

5.3 最佳匹配及其算法

先前两节讨论的都是边权为1的匹配问题，如果边权是非负实数，而且存在多个完全匹配，那么其中权和最大或最小的完全匹配就叫做最佳匹配。

例5.3.1 5项工作由5个人完成，如表所示。

$$C=\begin{bmatrix}3&4&6&4&9\\6&4&5&3&8\\7&5&3&4&2\\6&3&2&2&5\\8&4&5&4&7\end{bmatrix}$$

其中 C_{ij}表示 i 从事工作 j 的利润，如果每个人只做一项工作，那么最大的利润就应该是 $\max\Sigma c_{ij}$，c_{ij}不在相同的行与列。

假如 c_{ij}表示 i 从事工作 j 的成本，那么最小的成本应该是 $\min\Sigma c_{ij}$，c_{ij}不在相同的行与列。

显然这种最佳匹配就是二分图的最大权或最小权匹配。在讨论最佳匹配时，二分图 $G=(X,Y,E)$满足条件$|X|=|Y|$。

我们先介绍一个利用最小覆盖取代最大匹配的最大权匹配算法。

最大权匹配算法（已知利润矩阵C）。

1. 在矩阵C的每行选一最大值作为本行的界值 $l(x_i)$，每列的界值 $l(y_j)=0$。
   构造矩阵 $B=(b_{ij})_{n\times n}$，其中 $b_{ij}=l(x_i)+l(y_j)-c_{ij}$。
2. 在 B 中对0元素进行最小覆盖，覆盖数为 r。
   2.1 若 $r=n$，转4。
   2.2 在未覆盖的元素中选最小非零元，设值为 δ。
   若 x_i 行、y_j 列均已覆盖，则 $b_{ij}\leftarrow b_{ij}+\delta$。
   若 x_i 行、y_j 列均未覆盖，则 $b_{ij}\leftarrow b_{ij}-\delta$。
3. 修改界值
   若 x_i 行没覆盖，令 $l(x_i)\leftarrow l(x_i)-\delta$
   若 y_j 列已覆盖，令 $l(y_j)\leftarrow l(y_j)+\delta$
   删除覆盖标记，转2。
4. $\sum(l(x_i)+l(y_j))$即是最大权，结束。

例5.3.2 求例5.3.1表中的最大利润。

解：首先得到矩阵B，界值已在表的两旁标出，最小覆盖是1，5两列，$\delta=2$。

$$\begin{array}{c}\\9\\8\\7\\6\\8\\\\\end{array}\begin{array}{ccccc}\downarrow&&&&\downarrow\\ \left[\begin{array}{ccccc}6&5&3&5&0\\2&4&3&5&0\\0&2&4&3&5\\0&3&4&4&1\\0&4&3&4&1\end{array}\right]\\ 0\;\;0\;\;0\;\;0\;\;0\end{array}$$

$r<n$，B 中没覆盖的元素均减 δ；修改界值，结果如右。这时一个最小覆盖是第 1，5 列，第 3 行。$\delta=1$。

$$
\begin{array}{c|ccccc|}
 & \downarrow & & & & \downarrow \\
7 & 6 & 3 & 1 & 3 & 0 \\
6 & 2 & 2 & 1 & 3 & 0 \\
5 & 0 & 0 & 2 & 1 & 5 \\
4 & 0 & 1 & 2 & 2 & 1 \\
6 & 0 & 2 & 1 & 2 & 1 \\
 & 2 & 0 & 0 & 0 & 2
\end{array}
$$

$r<n$，B 中没覆盖元素减 1，双重覆盖元加 1。修改界值，这时一个最小覆盖是 1，2，3，5 列。$\delta=1$。

$$
\begin{array}{c|ccccc|}
 & \downarrow & \downarrow & \downarrow & & \downarrow \\
6 & 6 & 2 & 0 & 2 & 0 \\
5 & 2 & 1 & 0 & 2 & 0 \\
5 & 1 & 0 & 2 & 1 & 6 \\
3 & 0 & 0 & 1 & 1 & 1 \\
5 & 0 & 1 & 0 & 1 & 1 \\
 & 3 & 0 & 0 & 0 & 3
\end{array}
$$

$r<n$，B 中没覆盖元减 1，修改界值，这时的一个最小覆盖是第 3，4，5 行，3，5 列，最小覆盖数 $r=n$。一个最大权匹配方案是 $\{c_{13}, c_{25}, c_{34}, c_{42}, c_{51}\}$，$\sum(l(x_i)+l(y_j))=29$。结束。

$$
\begin{array}{c|ccccc|c}
 & & & \downarrow & & \downarrow & \\
5 & 6 & 2 & 0 & 1 & 0 & \\
4 & 2 & 1 & 0 & 1 & 0 & \\
4 & 1 & 0 & 2 & 0 & 6 & \leftarrow \\
2 & 0 & 0 & 1 & 0 & 1 & \leftarrow \\
4 & 0 & 1 & 0 & 0 & 1 & \leftarrow \\
 & 4 & 1 & 1 & 0 & 4 &
\end{array}
$$

定理 5.3.1 算法的结果是矩阵 C 的最大权匹配。

证明：所选取的矩阵 B 满足

$$b_{ij} = l(x_i) + l(y_j) - c_{ij} \geqslant 0. \tag{1}$$

设 W 是 C 的最大权匹配权和，一定有

$$\sum(l(x_i) + l(y_i)) \geqslant \max\sum c_{ij} = W。 \tag{2}$$

如果等式成立，那么一定存在 n 个不在同行同列的 c_{ij}，满足 $c_{ij}=l(x_i)+l(y_j)$，或者说 B 中有 n 个不在同行同列的 0 元素，处于这 n 个位置的 c_{ij} 构成了最大权匹配。如果最多存在 k $(<n)$ 个这样的 0 元素，(2)式就不可能相等，设此时的最小覆盖盖住了 c 行 d 列，其对应的结点集为 X_c 和 Y_d，由定理 5.2.3，$k=c+d<n$。令 B 中没被覆盖的最小元是 $\delta(>0)$，按照算法在修改界值时，对没覆盖的各行，令 $l^*(x_i)=l(x_i)-\delta$；对覆盖的各列，令 $l^*(y_j)=l(Y_j)+\delta$，其余界值不变。为了保证(1)式不变，即修改界值后仍需满足

$$b'_{ij} = l^*(x_i) + l^*(y_j) - c_{ij} \geqslant 0,$$

就应该对 b_{ij} 的不同位置分别作如下处理。

① 在覆盖的行和列的交叉点位置，

$$b_{ij}^* = l^*(x_i) + l^*(y_j) - c_{ij} = l(x_i) + l(y_j) + \delta - c_{ij} = b_{ij} + \delta,$$

② 没被覆盖，$b_{ij}^* = l(x_i) - \delta + l(y_j) - c_{ij} = b_{ij} - \delta$，

③ 只被行覆盖，$b_{ij}^* = l(x_i) + l(y_j) - c_{ij} = b_{ij}$，

④ 只被列覆盖，$b_{ij}^* = l(x_i) - \delta + l(y_j) + \delta - c_{ij} = b_{ij}$，

在上述每种情况下，$b_{ij}^* \geqslant 0$ 成立。综上，在对界值和元素 b_{ij} 修改之后，式(1)和(2)继续保持成立。但新的界值之和

$$\sum(l^*(x_i) + l^*(y_j)) = \sum(l(x_i) + l(y_j)) - \delta(n-c) + \delta d,$$

而

$$-\delta(n-c) + \delta d = \delta(c+d-n) < 0,$$

即界值之和下降。由于 δ 选值最小，因此它是最小下降。界值以及 b_{ij} 调整后，B 中出现了新的 0 元素，将可能增加最小覆盖数。经过若干次迭代之后，界值之和将恰好等于最大权匹配值。

如果矩阵 C 表示成本矩阵，那么它的最小权匹配或最小成本也就容易计算了。一种方法是确定一个 n 阶矩阵 $Q=(q_{ij})$，其中 q_{ij} 是一个大于等于 $\max c_{ij}$ 的常数 a，令 $C'=Q-C$，则 $c_{ij}+c_{ij}=a$。这样矩阵 C 的最小成本对应了 C' 的最大利润。对 C' 调用最大权匹配算法就容易计算 C 的最小成本。另一种方法类似于最大权匹配算法的思路。首先选每行的最小元为界值，满足 $b_{ij}=c_{ij}-l(x_i)-l(y_j)\geqslant 0$。然后不断最小地增加界值，直至存在 n 个不在同行同列值为 0 的 b_{ij} 出现。

例 5.3.3 求下表中的最小成本。

$$C = \begin{bmatrix} 7 & 6 & 4 & 6 & 1 \\ 4 & 6 & 5 & 7 & 2 \\ 3 & 5 & 7 & 6 & 8 \\ 4 & 7 & 8 & 8 & 5 \\ 2 & 6 & 5 & 6 & 3 \end{bmatrix}$$

解：选用 $a=10$，得到矩阵 $C'=(c'_{ij})$，$c'_{ij}=10-c_{ij}$。C' 恰是例 5.3.2 计算的矩阵，因此 C 的最小成本是：

$$5 \times 10 - \max \sum c'_{ij} = 21。$$

相应的一个最小权匹配方案是 $\{c_{13}, c_{25}, c_{34}, c_{42}, c_{51}\}$。

如果直接对 C 进行计算，过程可以如下：

首先得到矩阵 B，界值已标出，满足 $b_{ij}=c_{ij}-l(x_i)-l(y_j)$，最小覆盖是 1,5 列，$\delta=2$。

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 2 \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccc} \downarrow & & & & \downarrow \end{array} \\ \begin{bmatrix} 6 & 5 & 3 & 5 & 0 \\ 2 & 4 & 3 & 5 & 0 \\ 0 & 2 & 4 & 3 & 5 \\ 0 & 3 & 4 & 4 & 1 \\ 0 & 4 & 3 & 4 & 1 \end{bmatrix} \\ \begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \end{array} \end{array}$$

$r<n$。B 中没覆盖的元素均减 δ，行、列都盖住的加 δ 修改界值。没覆盖的行界值加 δ，覆盖的列界值减 δ。这时一个最小覆盖是第 1，5 列，第 3 行，$\delta=1$。

$$\begin{array}{c|ccccc|c}
 & \downarrow & & & & \downarrow & \\
3 & 6 & 3 & 1 & 3 & 0 & \\
4 & 2 & 2 & 1 & 3 & 0 & \\
5 & 0 & 0 & 2 & 1 & 5 & \leftarrow \\
6 & 0 & 1 & 2 & 2 & 1 & \\
4 & 0 & 2 & 1 & 2 & 1 & \\
 & -2 & 0 & 0 & 0 & -2 &
\end{array}$$

$r<n$。B 中没覆盖的元素均减 δ，修改界值如下，这时一个最小覆盖是 1，2，3，5 列，$\delta=1$。

$$\begin{array}{c|ccccc|}
 & \downarrow & \downarrow & \downarrow & & \downarrow \\
4 & 6 & 2 & 0 & 2 & 0 \\
5 & 2 & 1 & 0 & 2 & 0 \\
5 & 1 & 0 & 2 & 1 & 6 \\
7 & 0 & 0 & 1 & 1 & 1 \\
5 & 0 & 1 & 0 & 1 & 1 \\
 & -3 & 0 & 0 & 0 & -3
\end{array}$$

$r<n$。B 中没覆盖的元素均减 δ，修改界值，这时的一个最小覆盖是 3，4，5 行，3，5 列，最小覆盖数 $r=n$。一个最小权匹配方案是 $\{c_{13}, c_{25}, c_{34}, c_{42}, c_{51}\}$，$\sum(l(x_i)+l(y_j))=21$。结束。

$$\begin{array}{c|ccccc|c}
 & & & \downarrow & & \downarrow & \\
5 & 6 & 2 & 0 & 1 & 0 & \\
6 & 2 & 1 & 0 & 1 & 0 & \\
6 & 1 & 0 & 2 & 0 & 6 & \leftarrow \\
8 & 0 & 0 & 1 & 0 & 1 & \leftarrow \\
6 & 0 & 1 & 0 & 0 & 1 & \leftarrow \\
 & -4 & -1 & -1 & 0 & -4 &
\end{array}$$

不论计算最大权匹配还是最小权匹配，算法在计算当前的最大匹配时，都采用了求最小覆盖的办法。这对人工计算较为方便。但由计算机实现，当然要利用最大匹配算法，在这时，怎样决定界值的修改，便是最佳匹配算法的关键。这里介绍一种可行的方案。

对每一个矩阵 B，令其中 $b_{ij}=0$ 的元素集合为 E，可以得到相应的二分图 $G=(X, Y, E)$，调用最大匹配的匈牙利算法可以求出它的一个最大匹配。比如例 5.3.2 的第一个矩阵 B 对应的二分图如图 5.8(a)，其最大匹配是 $M=\{(x_1,y_5),(x_3,y_1)\}$。由定理 5.2.3，$r=s$，即其最小覆盖数是 $|M|$。换句话说，能够在 M 中找到 r 个 x_i 或 y_j，使得每条边都至少与其中某个结点相关联。不妨先从 M 中取出 r 个 x_i 构成集合 R，如果它恰好满足这一条件，那么盖住这 r 个 x_i 所在的行便盖住了 B 的全部零元素，它就是一个最小覆盖。否则一定存在某点 $x_k \notin R$，且它的每个邻点 $y_j \notin R$，由于 M 是最大匹配，所以 y_j 必有一邻点 $x_i \in R$，即 $(y_j, x_i) \in M$。这样，在 x_k 所在的全部交互道路（交互支）P 上，用 y_j 代替 x_i，记为 $R=R\oplus P$，它保证了 R 的元素数目不变，而且 x_k 所在的交互支里的每条边都与 R 中的某点关联。如果对每一个 $x_k \in X$ 都进行了上述处理，那么最终得到的 R 就对应了 G 的一个最小覆盖。

以 5.3.2 为例，我们按上述过程继续处理。

1. $M=\{(x_1,y_5),(x_3,y_1)\}$，

   $R=\{x_1,x_3\}$，

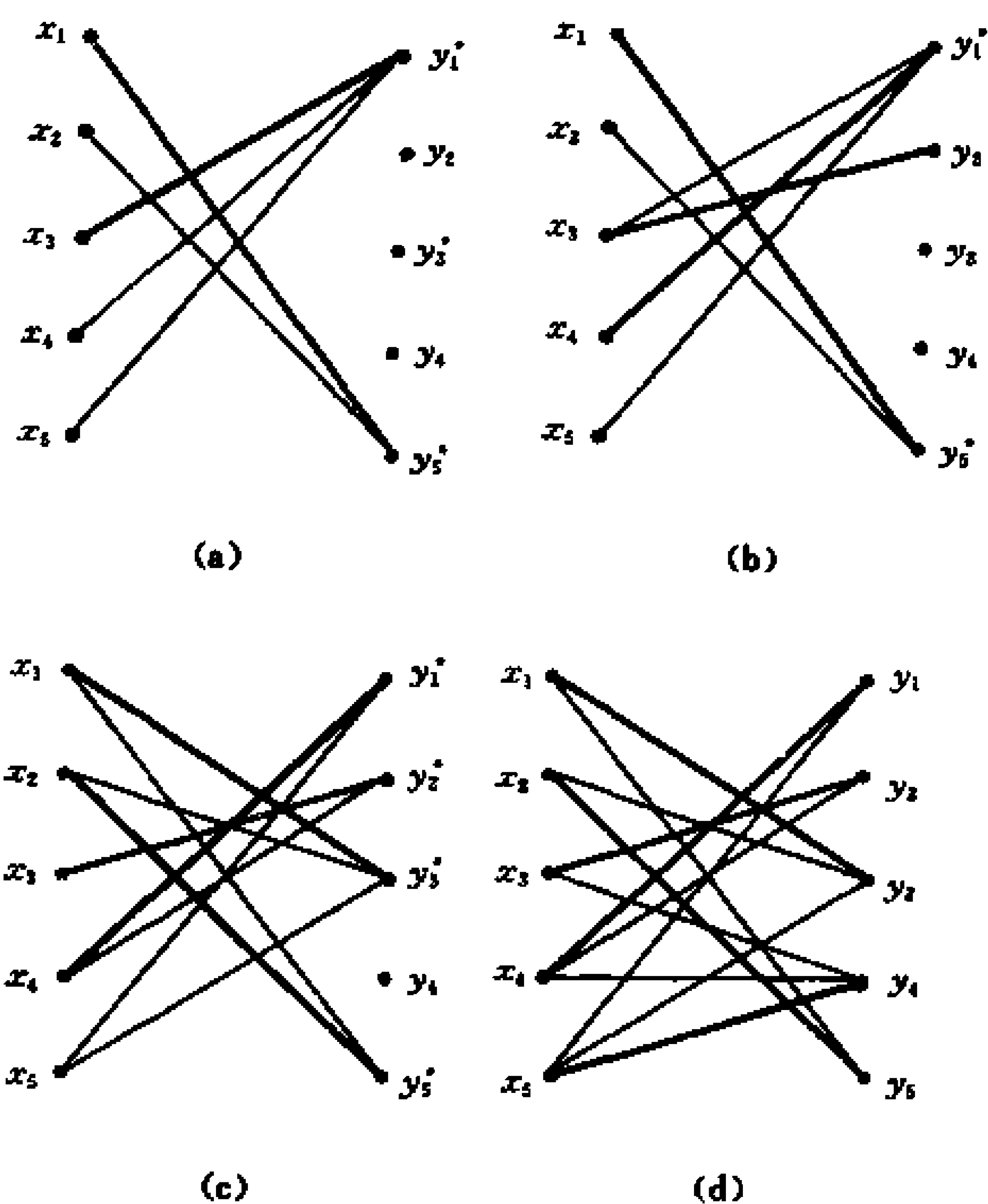


图 5.8

$x_2 \notin R \wedge \Gamma(x_2) \notin R$，

∴ $R = R \oplus P = R + y_5 - x_1 = \{x_3, y_5\}$。

$x_4 \notin R \wedge \Gamma(x_4) \notin R$。

∴ $R = R + y_1 - x_3 = \{y_5, y_1\}$。

2. $M = \{(x_1, y_5), (x_3, y_2), (x_4, y_1)\}$，

$R = \{x_1, x_3, x_4\}$，

∵ $x_2 \notin R \wedge \Gamma(x_2) \notin R$，

∴ $R = R + y_5 - x_1 = \{x_3, x_4, y_5\}$。

∵ $x_5 \notin R \wedge \Gamma(x_5) \notin R$，

∴ $R = R + y_1 - x_4 = \{x_3, y_5, y_1\}$。

3. $M = \{(x_1, y_3), (x_2, y_5), (x_4, y_1)\}$，

$R = \{x_1, x_2, x_3, x_4\}$，

$x_5 \notin R \wedge \Gamma(x_5) \notin R$，

x_5 所在交互支是 G，

∴ $R = R \oplus P = \{y_1, y_2, y_3, y_5\}$。

最小覆盖的问题一经解决，则界值以及 b_{ij} 的修改，进而新图 G 的产生就容易实现。此就不再多述。由于最小覆盖的计算量是 $O(n)$，最大匹配算法的计算复杂性是 $O(n^2)$，佳匹配最多需要迭代 n 次，所以它的计算复杂性是 $O(n^3)$。

5.4 最大基数匹配

一般图的最大匹配亦称为最大基数匹配。最大基数匹配算法的依据仍然是定理 5.1.1，即 M 是 G 的最大匹配，当且仅当 G 中不存在关于 M 的可增广路。但由于一般图既可能存在偶回路，也可能存在奇回路，它比二分图不存在奇回路的情况要复杂，因此最大基数匹配算法要考虑更一般的情形。

为了寻找关于匹配 M 的一条可增广交互道路，必须从某一个非饱和点 u 开始，如果存在一条 u 到 u' 的增广路 P，则在道路 P 中 u' 或是与 u 邻接，或是与另一饱和结点 v 邻接，且 v 与 u 的距离（即 u 到 v 这条道路所包含的边数）为偶数。这意味着，当且仅当存在与这样的结点 v 相邻的非饱和点 u'，才存在增广道路 $P(u,u')$.

例如，令 v_1，v_2，…，v_r 是与 u 邻接的点，如果其中之一是非饱和点，则我们就找到了一条增广路，否则，令 u_1，u_2'，…，u_r 是匹配 M 中它们相互配对的结点，取出其中一个结点，比如 u_1，找它的全部未查邻点，如果其中有一点是非饱和点，那么就得到了一条增广路。不然，在 M 中它们也有相配对的结点 u_1'，u_2'，…，u_r'。这种过程叫交互树的生长过程。非饱和点 u 称为根。

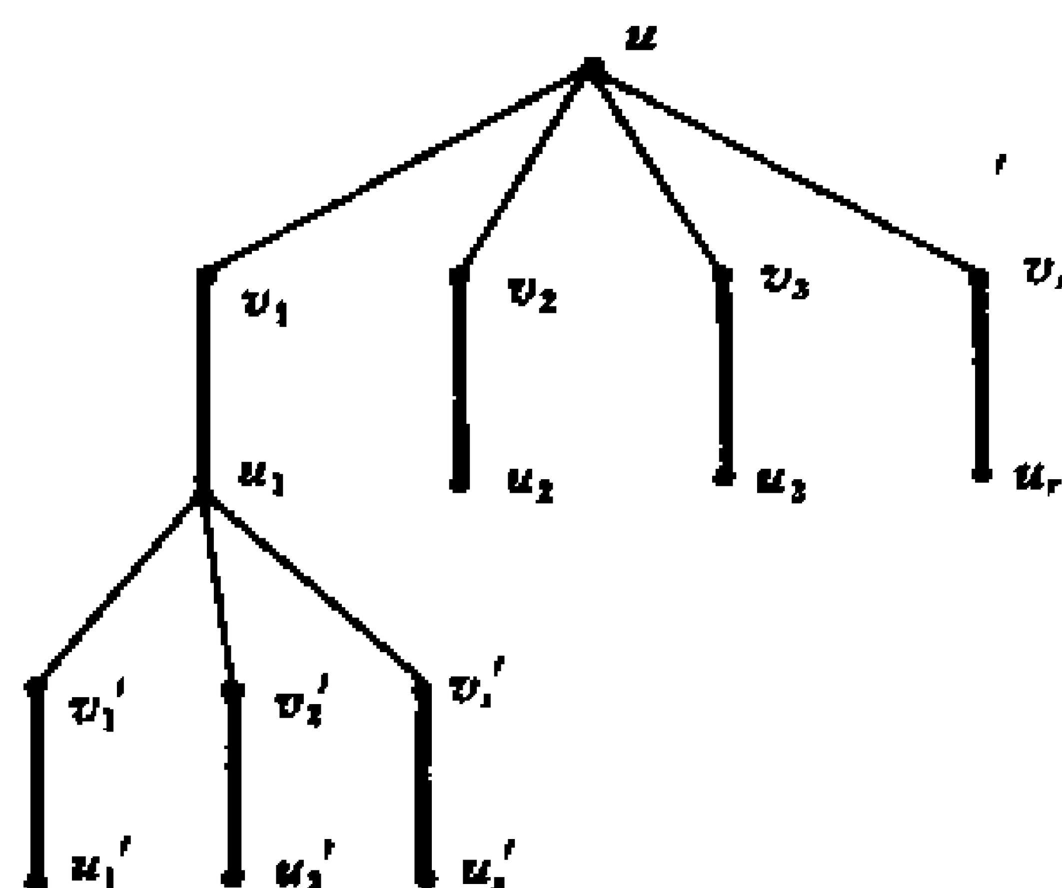


图 5.9

假定在离根 u 的距离为偶数的两个结点 u_i 和 u_j 亦是相邻接的，那么加入边 (u_i, u_j) 就构成了一个奇回路。比如图 5.9 中加入(u_1',u_2')就会形成奇回路$(u_1',u_2',v_2',u_1,v_1')$；加入$(u_r',u_3)$会形成奇回路$(u_r',u_3,v_3,u,v_1,u_1,v_r')$。

定义 5.4.1 在交互树生长中，若存在 $2k+1$ 个结点的奇回路 C，其中有 k 条边属于匹配 M，则称 C 是关于匹配 M 的一个树花，C 中唯一的非饱和点 v_0 称为花基。

比如上面两个树花中，u_1 和 u 分别是花基。

定理 5.4.1 树花上的任意一点到根 u 都存在距离是偶数的交互道路。

证明：由前述交互树的生长过程，花基到根的距离是偶数，而树花是一个奇回路，其中任一点到花基都有两条道路，其长度是一个为奇，另一个是偶。因此定理得证。

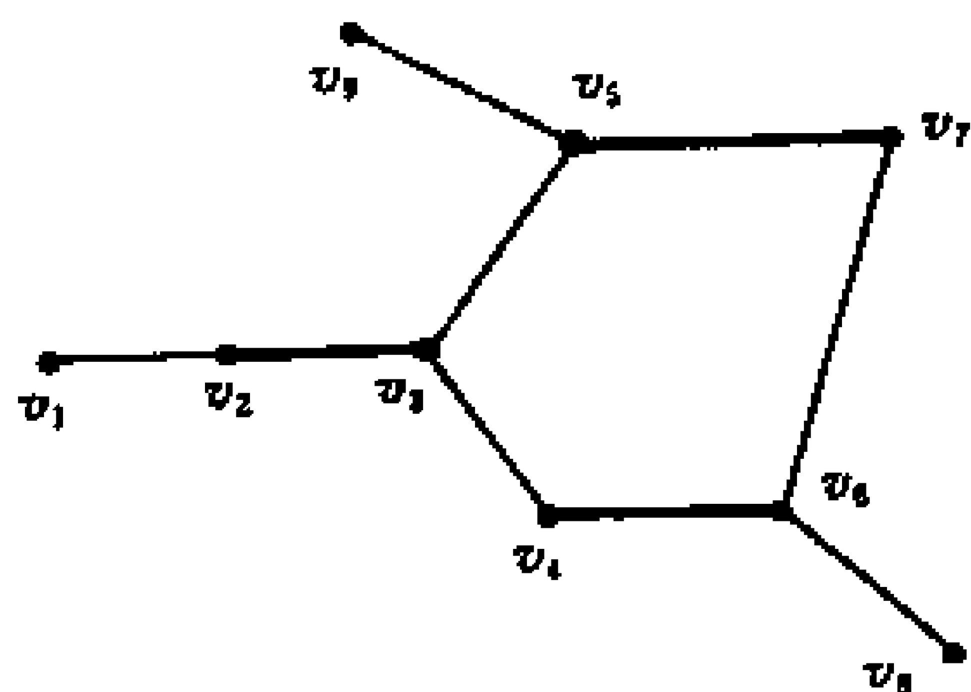


图 5.10

定理 5.4.1 说明树花上的任意结点，如果它有非饱和的未查邻接点 u'，那么一定存在 u 到 u' 的增广路。

例 5.4.1 设 $M=\{(v_2,v_3),(v_4,v_6),(v_5,v_7)\}$ 是图 5.10 的一个匹配，若从非饱和点 v_1 开始找增广路，则$(v_1,v_2,v_3,v_4,v_6,v_8)$是一条，$(v_1,v_2,v_3,v_4,v_6,v_7,v_5,v_9)$也是一条。其中 v_6，v_5 到 v_1 都存在偶长的交互道。但如果删去(v_6,v_7)，那么 v_5 到 v_1 就不存在偶长的路，

也就不会有 v_1 到 v_9 的增广路了。

爱德蒙茨(Edmonds)最先给出了最大基数匹配的算法，在其算法中一旦产生了树花，就用一个新结点代替这个树花中的全部结点。这个新结点称为伪点，原图中凡与该树花中某个结点邻接的点，现在都与该伪点相邻。这样得到了一个导出图。只要找到一个树花，这个过程就将重复。

如果在最终的导出图中仍没有增广路，这就意味着原图 G 关于非饱和点（根）u 不存在任何增广路，假如在某个导出图中找到了一条增广路，就意味着原图 G 存在与之对应的增广路，当然如果有伪点，需要把它先展开成树花，然后才能找到真正的增广路。当对所有的非饱和点 u 都进行了上述判断和修改后，M 就是最大基数匹配。

Edmonds 算法需要对树花进行收缩和展开，它的计算复杂性是 $O(n^4)$。盖宝(Gabow)提出一些技术，避免了树花的收缩和展开操作，从而使计算复杂性改进为 $O(n^3)$。我们重点介绍 Gabow 算法。

令图 G 有 n 个结点 m 条边，结点的编号为 1 到 n，而边的编号为 $n+2$，$n+4$，…，$n+2m$，边 (x,y) 的编号记为 $N(x,y)$。

EN 是一个数组。如果边 (v,w) 的编号是 k $(k=n+2i)$ 那么 $EN(k-1)=v$,$EN(k)=w$。

数组 MATE 存放匹配的边，如果 MATE$(v)=w$，MATE$(w)=v$，那么边 (v,w) 在匹配 M 中。

在从非饱和点 u 开始找交互道时，结点 v 称为外点，当且仅当 u 到 v 的距离是偶数。否则称为内点。很清楚，当交互道路 $P(v)$ 从 v 向 u 回溯时是从一条匹配边开始的，亦即若 $P(v)=(v,v_1,\cdots,u)$，那么边 (v,v_1) 是匹配边。

如果一个非饱和点 $u'(\neq u)$ 与某个外点 v 相邻，那么就得到了一条增广路

$$(u')*P(v)=(u',v,v_1,\cdots,u)$$

其中 * 表示联接。假如找不到这样的边 (u,v)，那么 u 不会处于一条增广路上。

LABEL 是一个 n 维向量，为每个结点提供一个存储单元，每个外点 v 可以用它来寻找一条交互道路 $P(v)$。

最初对非饱和点 u 有一个初始标号，LABEL$(u)=0$。这时的交互路是 $P(u)=u$。

结点标号。如果 LABEL$(v)=i$，$1\leqslant i\leqslant n$，称结点 v 有结点标号，此时说 v 是个外点，LABEL(v) 是另一个外点的结点号，交互道路 $P(v)$ 定义为 $(v,\text{MATE}(v))*P(\text{LABEL}(v))$。

边标号。如果 LABEL$(v)=n+2i$，$1\leqslant i\leqslant m$，称 v 有一个边标号，此时 v 也是一个外点，LABEL(v) 是连接两个外点，比如 x 和 y 的边号，即 LABEL$(v)=N(x,y)$。它表明外点 v 到根 u 的偶长交互路 $P(v)$ 必须经过边 (x,y)。这时 $P(v)$ 可以用 $P(x)$ 和 $P(y)$ 来表示：如果 v 处于 $P(x)$ 上，令 $P(x,v)$ 表示从 x 沿 $P(x)$ 到 v 的部分路径，那么 $P(v)=P^{-1}(x,v)*P(y)$，其中 $P^{-1}(x,v)$ 表示 $P(x,v)$ 的逆向。

LABEL$(v)<0$ 表示 v 不是外点。最初全部结点都看作是内点，并且 LABEL(v) 的赋值均为 -1。

数组 FIRST，如果 v 是一个外点，则 FIRST(v) 是 $P(v)$ 中的第一个内点，如果 v 是内

点，则 FIRST$(v)=0$。

数组 OUTER 用来存储在搜索增广路时遇到的外点。

Gabow 算法由下述三个过程组成：PROC-EDMONDS，PROC-LABEL 和 PROC-REMATCH。

PROC-EDMONDS 是主过程，它从每一个非饱和点开始搜索一条增广路。它扫描图 G 的边，决定标号的赋值。当检测到一条增广路后，调用过程 PROC-REMATCH，该过程将获得比原匹配多一条边的新匹配。如果产生树花，即扫描到两个外点 x, y 之间的一条边 (x, y) 时，将调用过程 PROC-LABEL。它将进行下述处理：

1. 变量 JOIN 的值置为花基结点，即路径 $P(x)$ 和 $P(y)$ 的第一个公共点的标号。

2. $P(x)$和 $P(y)$中 JOIN 之前的全部内点，即树花中的全部内点都改为外点。它们都赋值以边标号 $N(x,y)$，它指明凡经过这些结点的偶长交互道都必须通过边 (x, y)。

3. 树花中全部内点的 FIRST 值都置为 JOIN。

以下详细描述 Gabow 的最大基数匹配算法。

PROC-EDMONDS

E0. (初始化)将 G 的结点编号为 1 到 n，边编号为 $n+2, n+4, \cdots, n+2m$. 附加一个结点 0，对 $0 \leqslant i \leqslant n$，置 LABEL$(i)=-1$，FIRST$(i)=0$，MATE$(i)=0$，$u=0$。

E1. (找一个非饱和结点) 置 $u=u+1$，若 $u>n$ 则结束，此时 MATE 包含了一个最大基数匹配。否则若 u 是饱和点，转 $E1$。若 u 是非饱和点，把 u 送入数组 OUTER，置 LABEL$(u)=0$。

E2. (选择一条边) 用广探法选择一条尚未检查的边 (x, y)，其中 x 是外点。如果不存在这样的边，转 E7。

E3. (找到一条增广路) 如果 $y(\neq u)$ 是非饱和点，调用 PROC－REMATCH，转 E7。

E4. (形成树花) 如果 y 是外点，调用 PROC－LABEL，转 E2。

E5. (赋结点标号) 置 $v=$MATE(y)，若 v 是外点，转 E6；若 v 不是外点，置 LABEL$(v)=x$，FIRST$(v)=y$，并将 v 存入 OUTER 数组，转 E6。

E6. (得到下一条边) 转 E2。

E7. (停止搜索) 置 LABEL$(i)=-10$　$0 \leqslant i \leqslant n$，转 E1。

PROC-LABEL

L0. (初始化) 置 $r=$FIRST(x)，$s=$FIRST(y)，若 $r=s$ 转 L6。(此时树花中没有内点) 否则给 r 和 s 标记。($L1$ 和 $L2$ 是寻找 $P(x)$和 $P(y)$的 JOIN)。

L1. 若 $s \neq 0$，交换 r 和 s。

L2. 置 $r=$FIRST (LABEL (MATE (r))) (r 是 $P(x)$或 $P(y)$中下一个内点)，若 r 未标记，给 r 标记并转 L1。

L3. (x 和 JOIN 以及 y 和 JOIN 间的内点都标以 $N(x,y)$)，置 $v=$FIRST(x)并转 L4；置 $v=$FIRST(y)并转 $L4$，转 L5。

L4. (标记内点 v) 若 $v \neq$JOIN，置 LABEL$(v)=N(x,y)$，FIRST$(v)=$JOIN，并将

v 送入数组 OUTER。置 v=FIRST(LABEL(MATE(v)))。重复 $L4$ 直至 v=JOIN，返回 L3。

L5.（修改 FIRST）对每个外点 i，如果 FIRST(i)是外点，置 FIRST(i)=JOIN。

L6.（边标记结束）返回。

PROC-REMATCH

R0.（得到一条增广路）计算 $P(x)$如下：

1. 若 x 有一个边标号 $N(v,w)$，则计算 $P(v)$和 $P(w)$。如果 x 处于 $P(v)$之中，则

$$P(x)=P^{-1}(v,x)*P(w),$$

否则

$$P(x)=P^{-1}(w,x)*P(v)。$$

2. 若 x 有一结点标号，则

$$P(x)=(x,\text{MATE}(x))*P(\text{LABEL}(x)),$$

增广路径 P_a 是

$$P_a=(y)*P(x)。$$

R1.（修改匹配）令 $M=M\oplus P_a$，修改 MATE 数组，返回。

例 5.4.2 对图 5.11，设初始匹配由其中粗线边表示，Gabow 算法过程如下。

首先选中一个非饱和点 10，检索到的外点依次是 10，16，13，11，2。相应得到的以 10 为根的交互树如图 5.12，此时数组 LABEL 和 FIRST 的值如下表所示，OUTER 中包含的结点依次是 10，16，13，11，2，6 和 9。

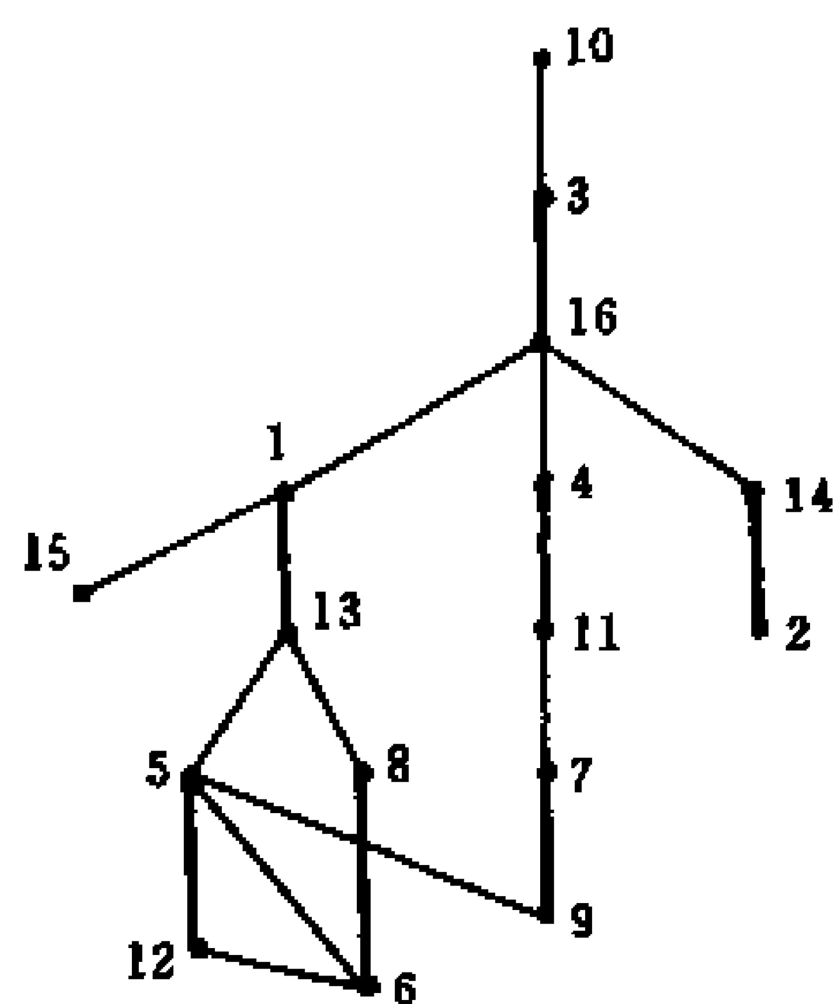


图 5.11

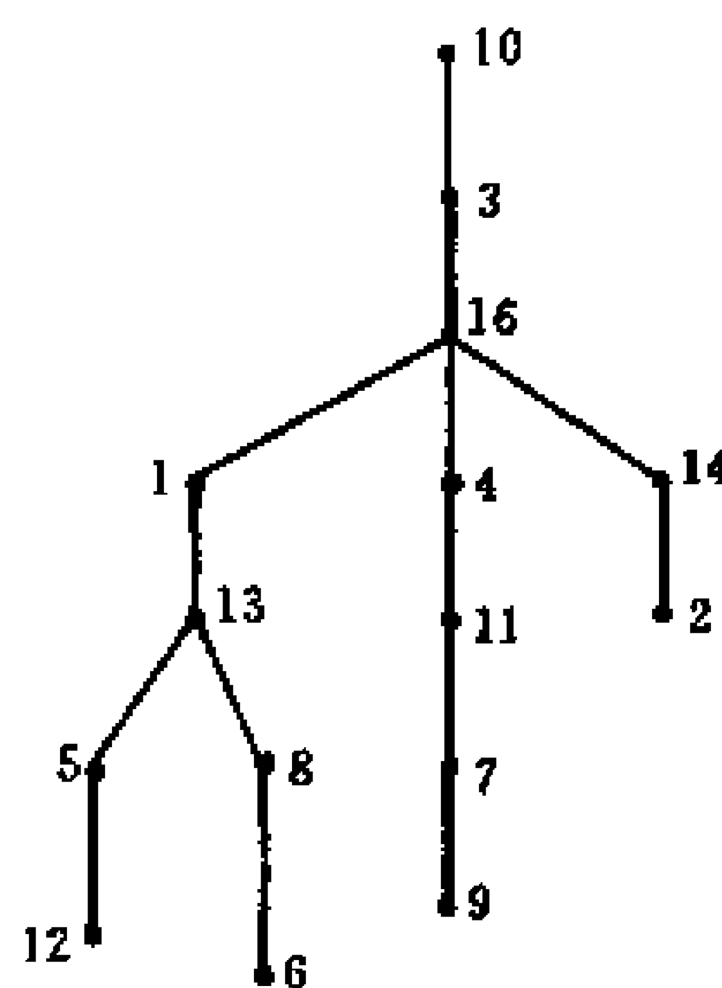


图 5.12

结点号	LABEL	FIRST	结点号	LABEL	FIRST	结点号	LABEL	FIRST	结点号	LABEL	FIRST
1	−1	0	5	−1	0	9	11	7	13	16	1
2	16	14	6	13	8	10	0	0	14	−1	0
3	−1	0	7	−1	0	11	16	4	15	−1	0
4	−1	0	8	−1	0	12	13	5	16	10	3

当从结点 12 向前搜索时，检索了边（12，6），得到树花（13，5，12，6，8），此时 LABEL 和 FIRST 变化如下：

LABEL (5) =LABEL (8) =N (12, 6),

FIRST (i) =1, i=5, 12, 6, 8。

结点 5 和 8 现在进入 OUTER 数组。

接着，当从结点 6 搜索时，检索到边 (6, 5)，由于它们的 FIRST 值相同，即已在一个树花内，所以不产生任何变化。于是再从结点 9 检索，查到边 (9, 5)，得到另一个树花 (9, 7, 11, 4, 16, 1, 13, 8, 6, 12, 5, 9)，再次改变 LABEL 和 FIRST 中这些结点的值如下：

结点号	LABEL	FIRST	结点号	LABEL	FIRST	结点号	LABEL	FIRST	结点号	LABEL	FIRST
1	N(9,5)	3	5	N(12,6)	3	9	11	3	13	16	3
2	16	14	6	13	3	10	0	0	14	−1	0
3	−1	0	7	N(9,5)	3	11	16	3	15	−1	0
4	N(9,5)	3	8	N(12,6)	3	12	13	3	16	10	3

现在数组 OUTER 中包含的结点依次是 10, 16, 13, 11, 2, 12, 6, 9, 5, 8, 1, 7 和 4，继续检查 9 以后的结点，对结点 5 和 8 的检查没有产生新的结点进入 OUTER，但查到 1 时，出现了边(1,15)，其中 15 是非饱和点，即找到了一条增广路，这条道路是 (15) * P(1)。

这时通过步骤 R0 计算 P(1)，结点 1 的 LABEL 值是 N(9,5)，因此需要知道 P(9)和 P(5)，而对结点 5，LABEL(5)=N(12,6)，所以又要知道 P(12)和 P(6)。

结点 12 有结点标号，所以

$$
\begin{aligned}
P(12) &= (12,\mathrm{MATE}(12)) * P(\mathrm{LABEL}(12)) \\
&= (12,5) * P(13) \\
&= (12,5) * (13,\mathrm{MATE}(13)) * P(\mathrm{LABEL}(13)) \\
&= (12,5,13,1) * P(16) \\
&= (12,5,13,1) * (16,\mathrm{MATE}(16)) * P(\mathrm{LABEL}(16)) \\
&= (12,5,13,1,16,3,10)。
\end{aligned}
$$

类似地

$$P(6) = (6,8,13,1,16,3,10),$$

$$P(9) = (9,7,11,4,16,3,10)。$$

因此结点 5 处于 P(12) 上。

$$
\begin{aligned}
P(5) &= (P^{-1}(12,5)) * P(6) \\
&= (5,12) * (6,8,13,1,16,3,10) \\
&= (5,12,6,8,13,1,16,3,10)。
\end{aligned}
$$

结点 1 处于 P(5)，所以

$$
\begin{aligned}
P(1) &= P^{-1}(5,1) * P(9) \\
&= (1,13,8,6,12,5,) * (9,7,11,4,16,3,10, \\
&= (1,13,8,6,12,5,9,7,11,4,16,3,10)。
\end{aligned}
$$

从增广路(15) * P(1)，我们可以得到 G 的更大匹配(15,1),(13,8),(6,12),(5,9),(7,11),(4,16),(3,10)和(14,2)，实际上它已经是最大匹配。

5.5 网络流图

定义 5.5.1 一个运输网络 N（或称网络流图）是一个没有自环的有向连通图。它满足

1. 只有一个负度为零的结点 s，称为源。

2. 只有一个正度为零的结点 t，称为汇。

3. 每条边 (i, j) 都有一个非负实数权 c_{ij}，称为该边的容量。如果结点 i 到 j 没有边，则 $c_{ij}=0$。

这种网络可以看成某种产品从产地 s 通过不同的道路可达销地，边的容量表示沿这条边最多能通过的量。图 5.13 就是一个网络流图。

图 5.13

在网络流图 N 中，如果每条边 e_{ij} 都给定一个非负实数 f_{ij}，满足

1. $f_{ij}\leqslant c_{ij}$，　　　　$e_{ij}\in N$。

2. $\sum\limits_{j} f_{ij}=\sum\limits_{j} f_{ji}$，　　$i\neq s, t$。

3. $\sum\limits_{j} f_{sj}=\sum\limits_{j} f_{jt}=w$。

那么这一组 f_{ij} 就叫做该网络的容许流，w 称为它的流量。在网络 N 的一个容许流分布 f 里，满足 $f_{ij}=c_{ij}$ 的边称为饱和边，否则是非饱和边。如果一个容许流分布使得网络的流量 w_0 为极大，即

$$w_0=\max\sum_{j} f_{sj},$$

就说 w_0 是网络的最大流。

对于多产地多销地的网络，可以再增加一个超发点 s_0 和超收点 t_0，增加若干条边 (s_0, s_i) 和 (t_j, t_0)，其中 s_i，t_j 分别是每个产地和销地，同时边 (s_0, s_i) 的容量是 s_i 的生产能力，(t_j, t_0) 的容量是 t_j 的销售能力。这样就得到了一个网络流图，即单源单汇的图。如图 5.14 所示意。

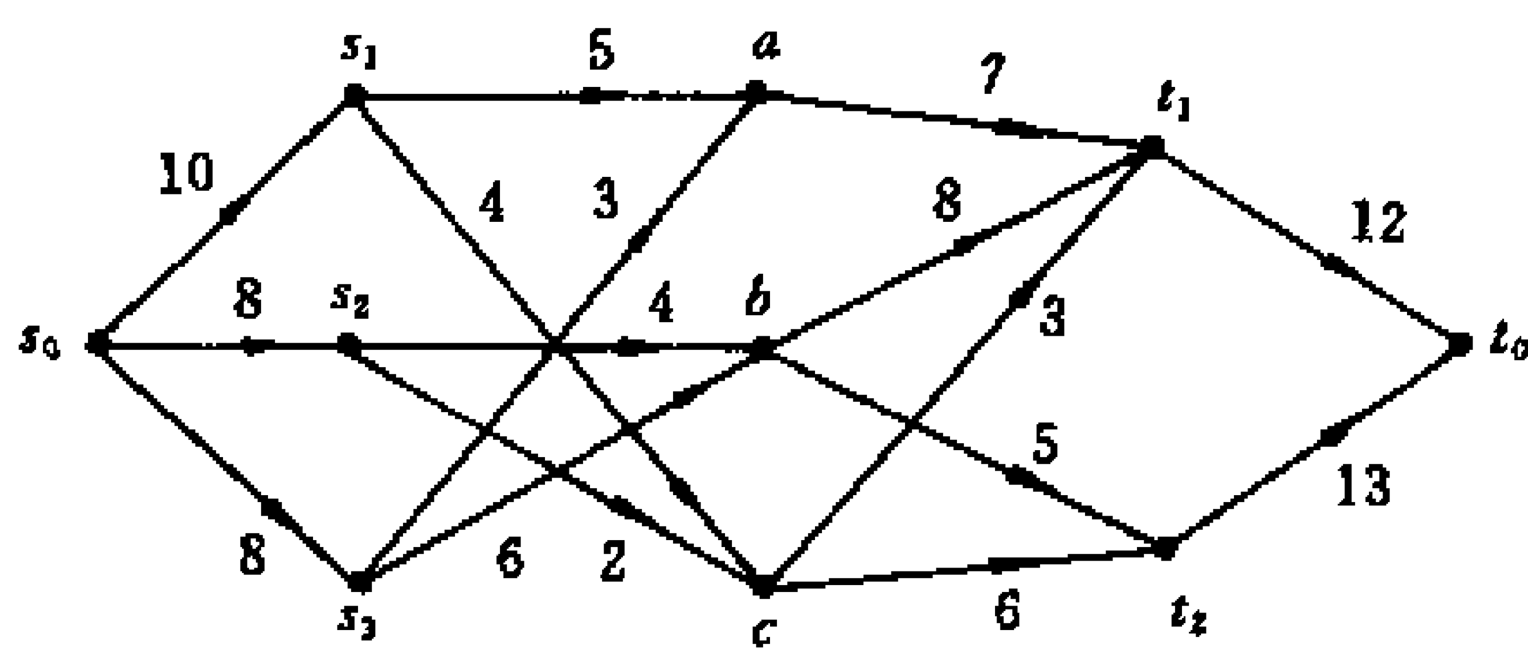


图 5.14

定义 5.5.2 设 S 是网络流图 $N=(V,E)$ 中的一个结点集，满足

1. $s\in S$。

2. $t\in\overline{S}$，$\overline{S}=V-S$。

则全部有向边 (i, j)，$i\in S$，$j\in\overline{S}$，的集合称为 N 的一个割切，记为 $(S, \overline{S})$，$(S, \overline{S})$ 中各边的容量之和称为该割切的容量，记为 $C(S, \overline{S})$，即

$$C(S,\overline{S}) = \sum_{(i,j)\in(S,\overline{S})} c_{ij}。$$

一般情况下，不同的割切有不同的割切容量。

例 5.5.1 图 5.13 中，令 $S=\{s\}$，则 $(S,\overline{S})=\{(s,a),(s,c),(s,d)\}$，$C(S,\overline{S})=6$。令 $S=\{s,a,c\}$，则 $(S,\overline{S})=\{(a,b),(c,b),(c,d),(c,t)(s,d)\}$，$C(S,\overline{S})=11$。

网络的流量与割切容量之间存在下述关系。

定理 5.5.1 网络的最大流量小于等于最小的割切容量，即

$$\max w \leqslant \min C(S,\overline{S})。$$

证明：设 f 是给定网络的任一容许流分布，由容许流的性质

$$\sum_j f_{sj} = w。\tag{1}$$

$$\sum_j (f_{ij} - f_{ji}) = 0。\quad i \neq s.t, j \in V。\tag{2}$$

任给一个割切 $(S, \overline{S})$，满足 $s\in S$，$t\in\overline{S}$ 由(1)，(2)式

$$\sum_{\substack{i\in s\\ j\in v}} (f_{ij} - f_{ji}) = w,$$

亦即

$$\sum_{\substack{i\in s\\ j\in s}} (f_{ij} - f_{ji}) + \sum_{\substack{i\in s\\ j\in \overline{s}}} (f_{ij} - f_{ji}) = w。$$

其中

$$\sum_{\substack{i\in s\\ j\in s}} (f_{ij} - f_{ji}) = 0,$$

因此

$$\sum_{\substack{i\in s\\ j\in \overline{s}}} (f_{ij} - f_{ji}) = w。$$

由于

$$0 \leqslant f_{ij} \leqslant c_{ij}, \qquad 且\ f_{ij} - f_{ji} \leqslant f_{ij},$$

所以

$$w = \sum_{\substack{i\in s\\ j\in \overline{s}}} (f_{ij} - f_{ji}) \leqslant \sum_{\substack{i\in s\\ j\in \overline{s}}} f_{ij} \leqslant \sum_{\substack{i\in s\\ j\in \overline{s}}} c_{ij} = C(S,\overline{S})。$$

由于容许流分布与割切 $(S, \overline{S})$ 的任意性，因此定理得证。

如果网络的容许流并不是最大流，就一定存在着从 s 到 t 的增流路径。怎样的路径才是增流路径呢？

令 s，i_1，i_2，…，i_k，t 是一条 s 到 t 的路径 P_{st}，其中每条边的方向都是从 i_j 到 i_{j+1}，称为向前边。如果这条路径上每条边 e_{ij} 都有 $f_{ij}<c_{ij}$，那么令 $\delta=\min\limits_{e_{ij}\in P_{st}} (c_{ij}-f_{ij})$，这时令 p_{st} 每条边的流都增加 δ，结果仍然是网络的容许流分布，但流量比先前增加了 δ。例如图 5.15 表示在网络 N 中某个容许流分布下的一条 P_{st} 道路，它全部由向前边组成，其中每条边有两个权值 (a, b)，a 表示其容量，b 表示它当前的流。显见该道路上 $\delta=1$，即沿这条 $s-t$ 道路网络的流量最多可增加 1。

除了全部由向前边组成的增流路径之外，还可以有包含向后边的增流路径 P_{st}，在这

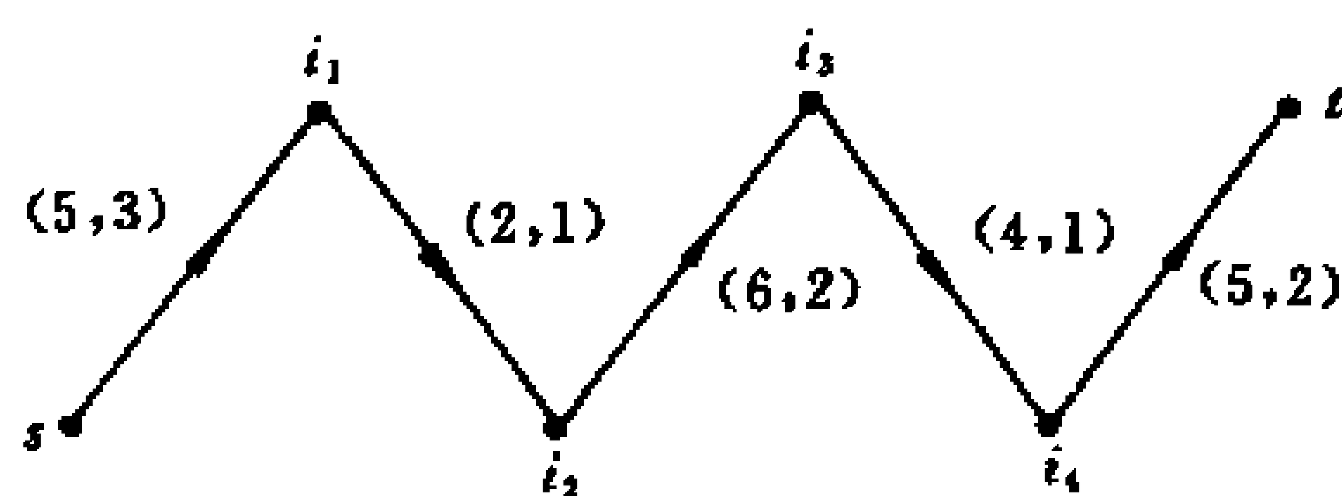


图 5.1

种路径中，要求向前边 e_{ij} 满足 $f_{ij}<c_{ij}$，向后边 e_{ji} 满足 $f_{ji}>0$，如图 5.16 所示。设 P_{st} 的全部向前边 e_{ij} 中，$\delta_1=\min(c_{ij}-f_{ij})$；全部向后边 e_{ji} 中，$\delta_2=\min f_{ji}$，再令 $\delta=\min(\delta_1,\delta_2)$，那么 P_{st} 中可增加流量 δ。比如图 5.16 的 $\delta=1$，在这条道路上的增流过程是这样的：汇点 t 的流入量增加 1 是从 i_4 获得，i_4 要保持流的守恒，应使 f_{34} 增加 1；而 i_3 的守恒是由 i_3 少供应 i_2 1 个单位流而得到保证，因此增流路径中的向后边 e_{ji} 一定要 $f_{ji}>0$，这时 i_2 由于 i_3 少供应 1，因此只有从 i_1 多索取 1 才能保持守恒。

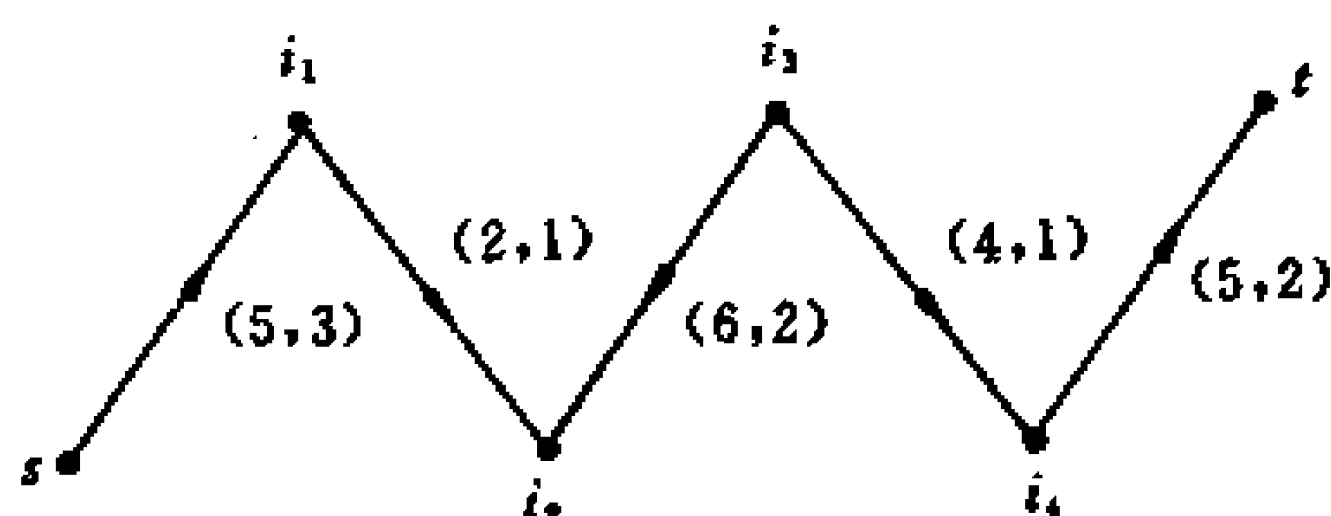


图 5.16

在网络流图中只存在上述两类增流路径。

例 5.5.2 图 5.17 中，如果最初流量 $w=0$，第一条增流路径可以是 (s, c, b, t)，它全部由向前边组成，$\delta=2$，因此可增流 2，这时边 (s, c)，(c, b)，(b, t) 的流都是 2，其余边均为 0，这是一个容许流分布。此时还存在另一条增流路 (s, a, b, c, d, t)，其中 (c, b) 是向后边，$f_{cb}=2$，其余边都是向前边，满足 $f_{ij}<c_{ij}$，这条路上 $\delta=1$，因此增流之后得到图 5.18。其中边 (c, b) 的流为 1，这仍然是一个容许流分布。此时网络中已不存在任何增流路径。所以最大流量是 $w_0=3$。

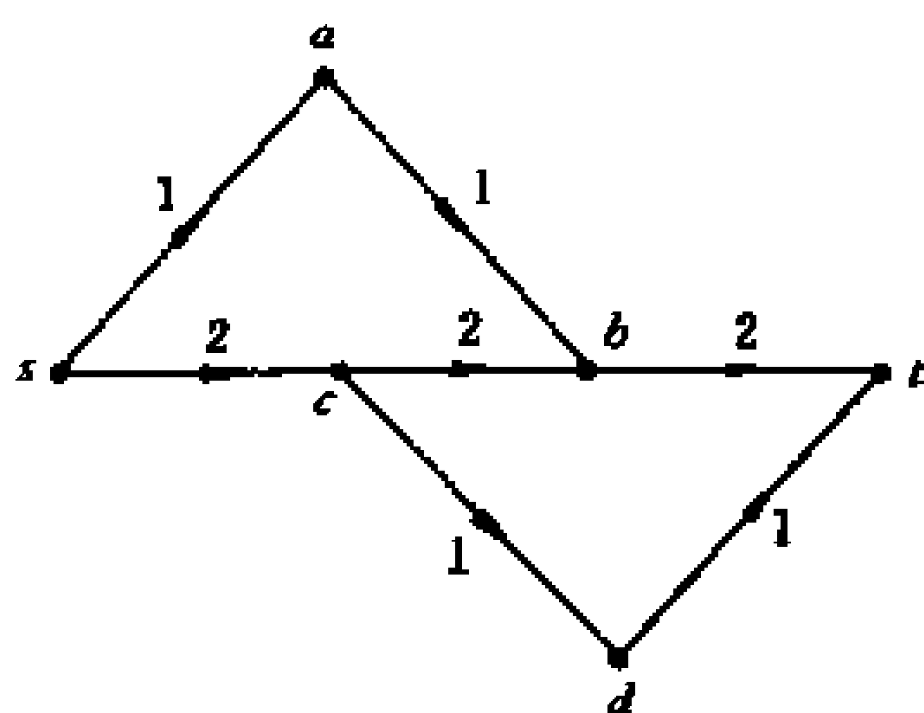


图 5.17

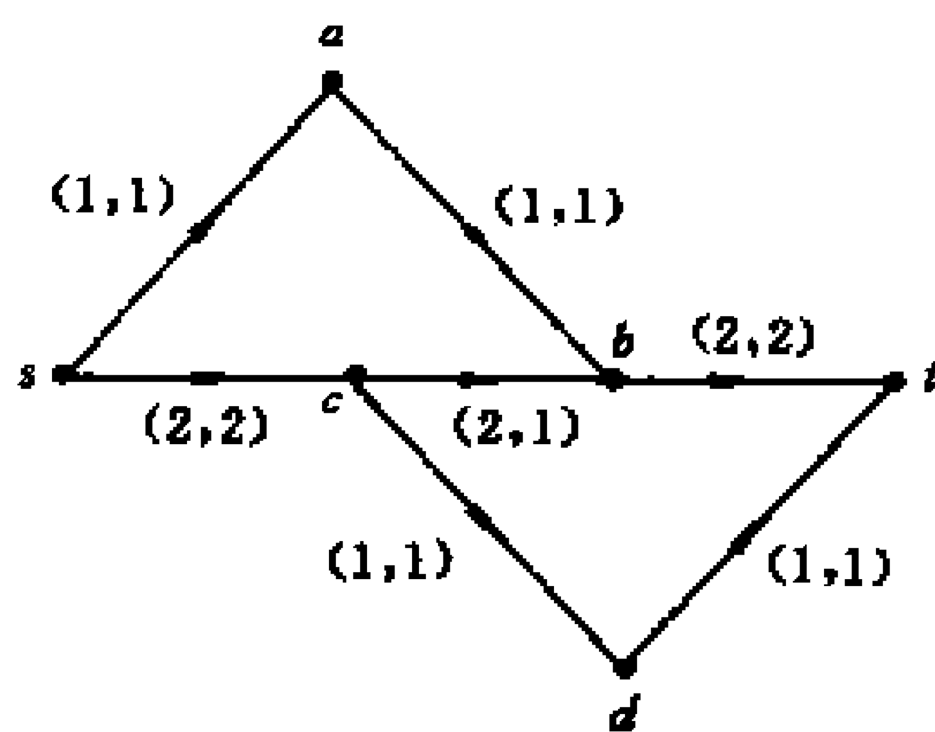


图 5.18

定理 5.5.2 网络流图 N 中，其最大流量等于其最小割切的容量。即

$$\max w = \min C(S, \overline{S})。$$

证明：设网络的一个容许流分布 f 已使得该网络的流量达到最大，确定一个割切 $(S, \overline{S})$ 如下：

1. $s\in S$。

2. 若 $x\in S$，(x,y) 是向前边且 $f_{xy}<c_{xy}$，则 $y\in S$。若 $x\in S$，(y,x) 是向后边且 $f_{yx}>$

0，则 $y \in S$。此时，必有 $t \notin S$，否则存在 s 到 t 的一条增流路径，与 f 是最大流分布矛盾。因此 $\bar{S} \neq \Phi$，根据上述定义，对任意满足 $x \in S, y \in \bar{S}$ 的边 (x,y)，若 (x,y) 是向前边，必有 $f_{xy} = c_{xy}$；若 (y,x) 是向后边，亦必定 $f_{yx}=0$，由定理 5.5.1，$\max w \leqslant \min C(S,\bar{S})$，但此时的流量 w 又满足

$$w = \sum_{\substack{x \in s \\ y \in \bar{S}}} (f_{xy} - f_{yx}) = \sum_{\substack{x \in s \\ y \in \bar{S}}} c_{ij} = C(S,\bar{S}),$$

亦即

$$\max w = \min C(S,\bar{S})。$$

5.6 Ford-Fulkerson 最大流标号算法

福特和富尔克逊 (Ford and Fulkerson) 最先给出了计算运输网络最大流量的标号算法，它以定理 5.5.2 为基础，包含了两个过程。

任意给定了网络的一个容许流分布 f 后，第一个过程称为标号过程，它检查网络中是否存在关于 f 的增流路径。如果不存在，则由定理 5.5.2，此时的 f 是最大流分布，其流量 w 为最大流。否则，在标号过程中最后能标到结点 t，即存在 s 到 t 的增流路径。这时便进入第二个过程：增流过程。在增流过程中，将确定一条 s 到 t 的增流路并修正这条路上的流。得到新的容许流分布 f'，再继续执行标号过程。

在标号过程里，每个结点 v 都有一组标号 (d_v,δ_v)，d_v 表示在标号过程里结点 v 是因为哪个结点才得到标号的，它也表示标号的方向，即是正向的还是反向的。如果 v 得到标号，就表明网络里存在一条 s 到 v 的增流路径 P，其最大的增流量是 δ_v。

在标号时，首先对源 s 标以 $(-,\infty)$，其中 d_s 的值无关紧要，则标号规则是：设 e 是连接 u 和 v 的边，假定 u 已经标号，而 v 尚未标号。

正向标号：如果 $e=(u,v)$ 且 $f(e)<c(e)$，则标号方向为正，v 得到标号 (u^+,δ_v)，其中

$$\delta_v = \min(\delta_u, c(e) - f(e))。$$

反向标号：如果 $e=(v,u)$ 且 $f(e)>0$，则标号为负，v 得到标号 (u^-,δ_v)，其中

$$\delta_v = \min(\delta_u, f(e))。$$

在标号过程中，每个结点最多进行一次标号，最终结点 t 或者能得到标号，或者无法得到标号。

如果 t 得到标号，那么由标号规则可以确定一条 s 到 t 的增流路径 P_u，它可以增流 δ_t。在增流过程里利用 d_v 可以回溯检索这条道路 P_u，同时修改每条边的流，得到新的容许流分布 f'。

Ford-Fulkerson 算法描述如下：

S1. 在给定的网络流图中任选一个容许流分布 f，可以令 N 中每条边 e，都有 $f(e) = 0$。

S2. (标号过程开始) 给 S 标号 $(-,\infty)$。

S3. 如果存在一个未标结点 v，它可以通过正向标号或反向标号得到标号，则标之并转 S4，否则转 S7。

S4. 如果 $v=t$ 转 S5，否则转 S3。

S5.（增流过程开始），设 v 的标号是(d_v,δ_v)。

1. 若 $d_v=u^+$，则令 $f(u,v)=f(u,v)+\delta_t$。
2. 若 $d_v=u^-$，则令 $f(v,u)=f(v,u)-\delta_t$。

S6. 如果 $u=s$，删去全部标号并转 S2，否则令 $v=u$，转 S5。

S7.（此时 f 已是最大流分布）结束。

下面举例说明这个算法。

例 5.6.1 图 5.19 是一个运输网络 N，每条边 e 都有两个权，依次是$c(e)$和$f(e)$，最初 N 中每条边 e 都是 $f(e)=0$，亦即流量 $w=0$。开始标号时结点 s 为$(-,\infty)$，之后依次给结点 a，b，c，d 和 t 的标号，结果如图所示。此时标号过程结束。在增流过程中我们将确定增流路径 P_{st}并修正容许流 f。

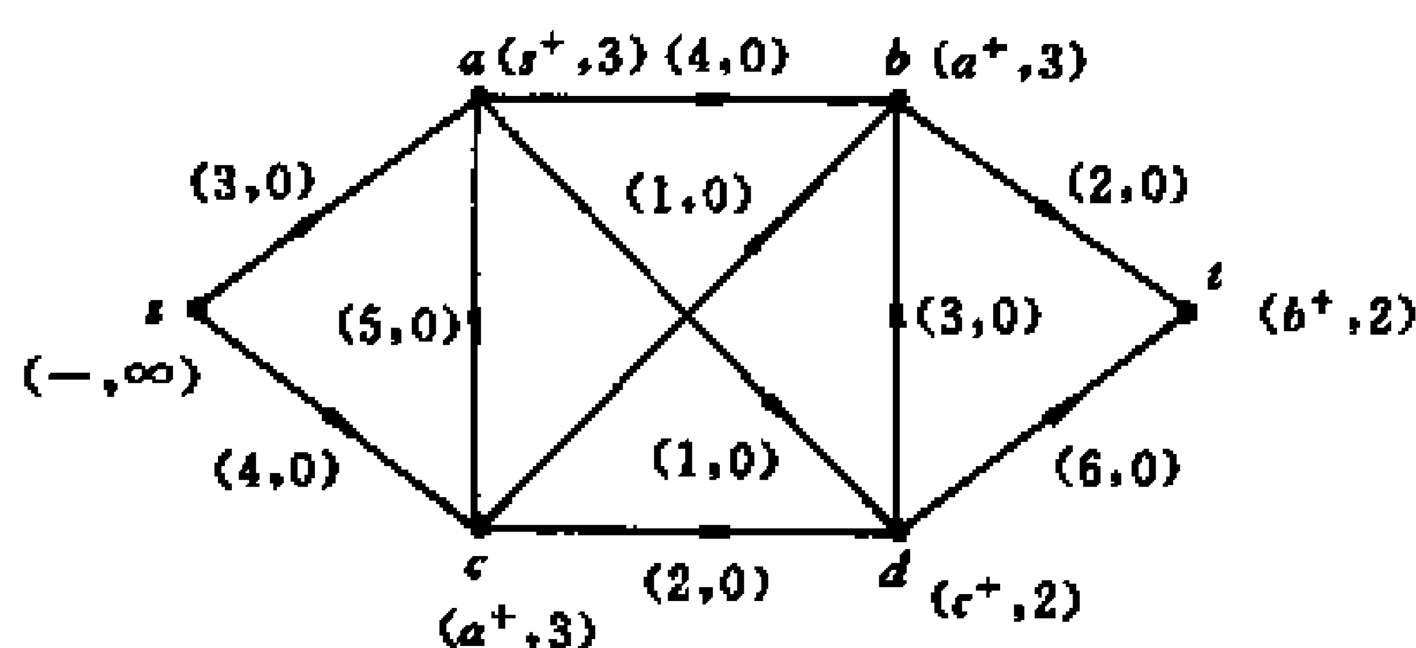


图 5.19

由 t 的标号 b^+表示这条 P_{st}路径中 t 的前趋是 b，类似地，由 b 的标号 a^-和 a 的标号 s^+可知这条路径是

$$s\to a\to b\to t,$$

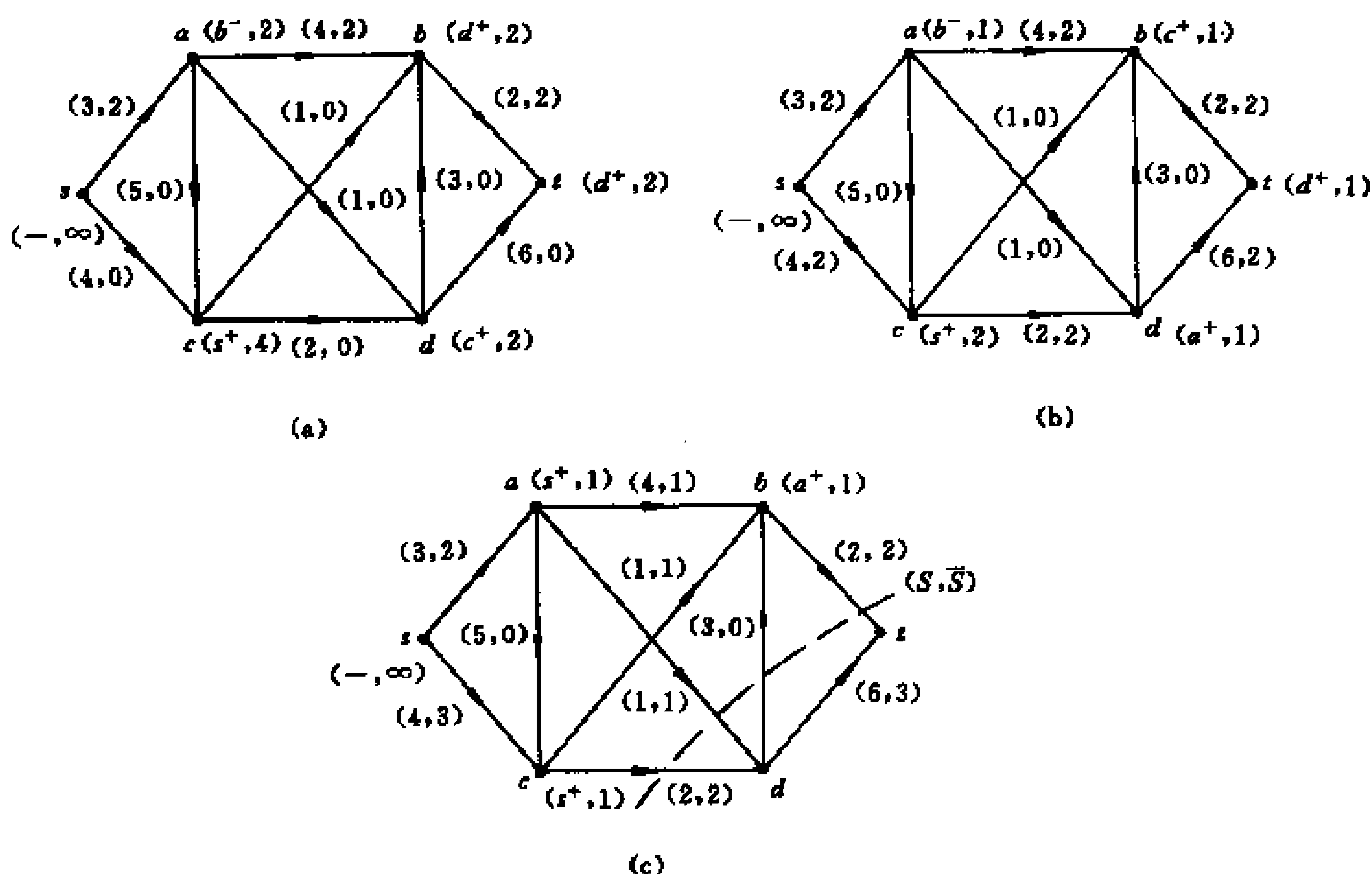


图 5.20

而且所有的边都是向前边，每条边的流都增加 $\delta_t=2$，这时网络流量 $w=2$，如图 5.20 (a)所示。

删去所有标号，从 S 开始重新标号如 5.20 (a)，又得到了一条增流路径 (s，c，d，

t)，可增流 $\delta_t=2$，此时 $w=4$。

以这时的容许流分布为基础的网络流图如 5.20 (b)，经过标号过程又得到一条增流路径 (s，c，b，a，d，t)，此时边 (a，b) 是向后边，其余都是向前边，这时向前边的流增 1 而向后边的流减 1，结果如图 5.20 (c)，$w=5$。

再从 S 开始标号，结果只能标到 a，c，b，而无法标到 d 和 t，因此不再存在 s 到 t 的增流路，$w=5$ 便是网络的最大流。令得到标号的结点属于 S，其余结点属于 $\overline{S}$，此时$(S,\overline{S})=\{(b,t),(a,d),(c,d)\}$，$C(S,\overline{S})=5$。满足定理 5.5.2。

5.7 最大流的 Edmonds-Karp 算法

上节描述的 Ford-Fulkerson 标号算法中，对结点的标号顺序是任意的，或者说如果存在的话，可以任意选择一条 s 到 t 的增流路径。这种特点，虽然有时会令人感到方便，但同时存在很严重的缺陷。

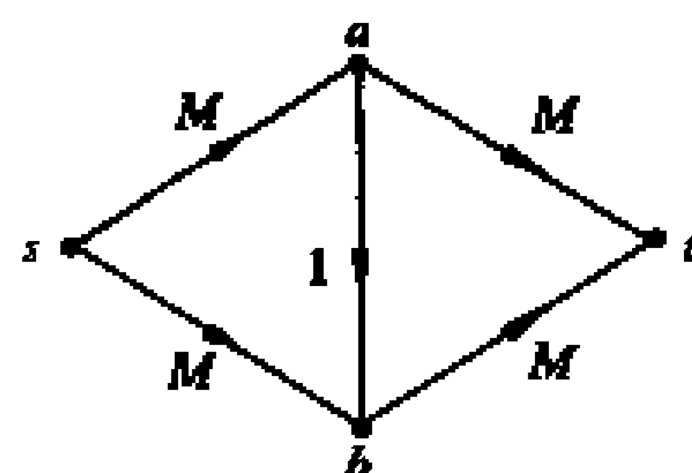


图 5.21

例 5.7.1 在计算图 5.21 的最大流中，采用标号法，可以先选择一条增流路 $P_1=$ (s，a，b，t)，增流 1；再选一条增流路 $P_2=$ (s，b，a，t)，增流量也是 1，然后交替选择 P_1 和 P_2，每次增流量都是 1。这完全符合 Ford-Fulkerson 标号算法，但总共要找 $2M$ 条增流路，其中 M 可以是任意正整数。这说明 Ford-fulkerson 算法的计算复杂性与问题的规模，即网络的结点数或边数无关，反而依赖某些任选的参数。

不仅如此，Ford 和 Fulkerson 也指出了当容量是无理数时他们的算法可能失效，并且举了一个例子，说明算法经过无限次才能收敛。

为了避免上述问题，艾德蒙兹和卡普 (Edmonds and Karp) 提出了一个严密的标号算法：在每一次都沿一条最短的增流路增流。所谓最短是指这条路包含的边数最少。显而易见，如果使用广探法，或者说先标号先检查的方法找到的一条 s 到 t 的增流路一定是最短的。Edmonds－Karp 算法对 Ford－fulkerson 算法的改动只有 S3 和 S4。

S3′ 按先标号先检查次序，选择标号最早但尚未检查的结点 u。

如果所有的结点都已检查，转 S7。否则对 u 的所有未标邻点 v，如果能通过正向或反向标号给以标号，则依次标之，转 S4′。

S4′ 如果 t 得到标号，令 $v=t$ 转 S5，否则转 S3′。

Edmonds-Karp 算法对原算法的改动虽小，却发生了质的变化。以图 5.21 为例，这时只有 2 条增流路径：$P_1=$ (s，a，t) 和 $P_2=$ (s，b，t)，分别增流 M 后即达到最大流分布。而且 Edmonds 和 Karp 证明了：改进算法的计算复杂性与边的容量无关。以下我们证明这一结果。

设 f 是网络 N 中容许流分布

$$P:\quad \underset{s=u_0}{\bullet}\overset{e_1}{\text{———}}\underset{u_1}{\bullet}\overset{e_2}{\text{———}}\underset{u_2}{\bullet}\cdots\cdots\underset{u_{i-1}}{\bullet}\overset{e_i}{\text{———}}\underset{u_i}{\bullet}\cdots\cdots\underset{u_{k-1}}{\bullet}\overset{e_k}{\text{———}}\underset{u_k=t}{\bullet}$$

是一条增流路。并令

$$\delta_i=\begin{cases}c(e_i)-f(e_i) & e_i\text{ 是向前边}\\ f(e_i) & e_i\text{ 是向后边}\end{cases}$$

$$\delta_t=\min\delta_i。$$

这时一定存在 i，满足 $\delta_i=\delta_t$，我们称 e_i 是该道路的瓶颈。假定标号法从初始流分布 f_0 开始，依照 Edmonds-Karp 算法依次构造容许流 f_1，f_2，…

如果向前边 e 是一条增流路 P 的瓶颈，那么在增流过程中它将饱和；如果这时 e 是向后边，则 $f(e)$将变为 0，显然可导致下述结论。

引理 5.7.1 若 $k<p$，且向前(后)边 e 是从 f_k 变为 f_{k+1}以及 f_p 变为 f_{p+1}时的瓶颈，则存在 l，满足 $k<l<p$，向后（前）边 e 是从 f_l 变为 f_{l+1}时增流路中的边。

令 $\lambda^i(u,v)$表示 f_i 中从 u 到 v 的一条最短非饱和路径长度，这时对其中的一条边 e，只有 $f_i(e)<c(e)$，它才能充当向前边；也只有 $f_i(e)>0$ 时它才可用作向后边。

引理 5.7.2 对每个结点 v 及每个 $k=0$，1，2…

$$\lambda^k(s,v)\leqslant\lambda^{k+1}(s,v)。\tag{1}$$

$$\lambda^k(v,t)\leqslant\lambda^{k+1}(v,t)。\tag{2}$$

证明：首先证明（1），若 f_{k+1}不存在 s 到 v 的非饱和路径，就令 $\lambda^{k+1}(s,v)=\infty$。上式成立。现假定

$$P:\quad \overset{e_1}{\underset{s=u_0}{\bullet\!\!-\!\!-}}\underset{u_1}{\bullet}\overset{e_2}{-\!\!-}\underset{u_2}{\bullet}\cdots\cdots\underset{u_{p-1}}{\bullet}\overset{e_p}{-\!\!-}\underset{u_p=v}{\bullet}$$

是 f_{k+1}中 s 到 v 的一条最短非饱和路。

如果 e_i 是 P 中的一条向前边，显然有 $f_{k+1}(e_i)<c(e_i)$，因此或有$(a)f_k(e_i)<c(e_i)$，或有$(b)f_k(e_i)=c(e_i)$，此时 e_i 已在 f_k 变为 f_{k+1}时充当了增流路中的向后边。

在情况(a)中，易见

$$\lambda^k(s,u_i)\leqslant\lambda^k(s,u_{i-1})+1。\tag{3}$$

而在情况(b)里

$$\lambda^k(s,u_{i-1})=\lambda^k(s,u_i)+1。$$

亦满足(3)式。

类似可证，如果 e_i 是 P 中的一条向后边，(3)式成立。

由于 $\lambda_k(s,u_0)=0$，因此对 $i=1,2,\cdots,P$，(3)式有

$$\lambda^k(s,u_p)\leqslant p=\lambda^{k+1}(s,v)。$$

同理可证(2)式。

引理 5.7.3 在采用先标号先检查原则求网络的最大流时，如果边 e 是从 f_k 变为 f_{k+1}时增流路中的一条向前(后)边，同时也是 f_l 变为 f_{l+1}时($k<l$)增流路的一条向后(前)边，则有

$$\lambda^l(s,t)\geqslant\lambda^k(s,t)+2。$$

证明：假定 e 是从 u 到 v 的边。由于 e 是 f_k 中的一条向前边，所以

$$\lambda^k(s,v)=\lambda^k(s,u)+1。\tag{4}$$

又由于 e 是 f_l 中的一条向后边，因此

$$\lambda^l(s,t) = \lambda^l(s,v) + 1 + \lambda^l(u,t)。\tag{5}$$

根据引理 5.7.2，有

$$\lambda^l(s,t) \geqslant \lambda^k(s,u) + \lambda^k(u,t) + 2 = \lambda^k(s,t) + 2。$$

这样我们可以得到

定理 5.7.1 如果在 Edmonds-Karp 标号算法中，每条增流路径都是当前最短的增流路，则网络中的增流路不超过 $m(n+2)/2$ 条。

证明：设边 e 的方向都是从 u 到 v，一个容许流序列是 f_{k1}，f_{k2}，…，其中 $k_1<k_2<\cdots$，而且边 e 在 f_{ki} 中是向前边瓶颈。由引理 5.7.1，存在另一个序列 l_1，l_2，…，满足

$$k_1 < l_1 < k_2 < l_2 < \cdots$$

且 e 在 f_{li} 中充当向后边。

由引理 5.7.3

$$\lambda^{k_i}(s,t) + 2 \leqslant \lambda^{l_i}(s,t),$$

同时

$$\lambda^{l_i}(s,t) + 2 \leqslant \lambda^{k_{i+1}}(s,t),$$

因此

$$\lambda^{k_1}(s,t) + 4(j-1) \leqslant \lambda^{k_j}(s,t)。$$

由于

$$\lambda^{k_j}(s,t) \leqslant n - 1,$$

$$\lambda^{k_1}(s,t) \geqslant 1,$$

所以

$$j \leqslant \frac{n+2}{4},$$

即 e 作为向前边最多能充当瓶颈 $(n+2)/4$ 次，类似地它作为向后边也最多只能充当瓶颈 $(n+2)/4$ 次，因此每条边最多只能充当 $(n+2)/2$ 次瓶颈，由于网络中有 m 条边，故增流路径最多有 $m(n+2)/2$ 条。

定理 5.7.2 Edmonds－Karp 最大流算法的计算复杂性是 $O(m^2n)$。

证明：使用先标号先检查方法，找一条增流路径最多检索 m 条边，由定理 5.7.1 即得证。

5.8 最 小 费 用 流

前面讨论了最大流问题，当时没有考虑每条边通过单位量的费用。本节我们将考虑在一个运输网络中，如果每条边都有其容量与单位量费用，怎样从源 s 以最小费用向汇 t 发送给定的流量 w。

例 5.8.1 一批货物要从工厂运至车站，可以有多条线路进行选择，在不同的线路上每吨货的运费不相同，而且每条线路的运货能力有限。这时怎样运输才能使运费最省？

用结点 s 代表工厂，t 表示车站，线路为边，线路的交点为网络的结点，每条边都有两个权：容量 c 和单位费用 a，于是构成网络流图 N，问题变为求 N 的最小费用流。

例 5.8.2 一个旅游社接待的一批客人第二天要从甲地飞到乙地，怎样安排才能使旅费最省？

这也是一个最小费用流问题，网络的结点是甲乙两地之间的各个机场，边表示第二

天的各个航班，其容量是该航班的有效座位数，而费用则是该航班的机票费。

设 $e=(i,j)$ 是网络流图 N 中的一条边，c_{ij} 表示该边的容量，a_{ij} 表示单位量的费用，f_{ij} 是当前该边的流，w 是要求从 s 到 t 的流量。于是最小费用流问题可以描述如下：

$$\min \sum_{e_{ij}} a_{ij} f_{ij}。$$

约束条件

$$0 \leqslant f_{ij} \leqslant c_{ij}。$$

$$\sum_j f_{ij} = \sum_j f_{ji}, \qquad i \neq s,t。$$

$$\sum_j f_{sj} = \sum_j f_{jt} = w。$$

最小费用流问题的一个好的有效算法是瑕疵(out of kilter)算法。它是 Ford 和 Fulkerson 首先提出来的。由于需要线性规划的知识，因此这里不再介绍。我们只讨论一种直观的但常常是有效的计算方法。

如果我们把费用看作是该边的长度，那么寻找一条从 s 到 t 的最短的增流路，它的费用增长得也就最小。如果最后的流量达到 w，这时的总费用一般应是最小。

最小费用流算法简单描述如下：

1. 初始流分布 f_0 使每条边 e 都为 $f(e)=0$，亦即 $w_0=0$。

2. 在当前的容许流分布下修改各边 (i,j) 的费用 a_{ij}^*，

$$a_{ij}^* = a_{ij}, \qquad 0 \leqslant f_{ij} < c_{ij}。$$

$$a_{ij}^* = \infty, \qquad f_{ij} = c_{ij}。$$

$$a_{ij}^* = -a_{ji}, \qquad f_{ji} > 0。$$

3. 以 a_{ij}^* 为边长，找一条从 s 到 t 的最短增流路，得到增流量 δ_t。

4. 若 $\delta_t + w_0 \geqslant w$，则 $\delta_t \leftarrow w - w_0$，转 5，结束。否则转 5，转 2。

5. 增流过程。由 δ_t 修改容许流，返回。

算法中的增流过程与最大流算法是一样的，最短增流路可以先求其最短路，然后再计算 δ_t。

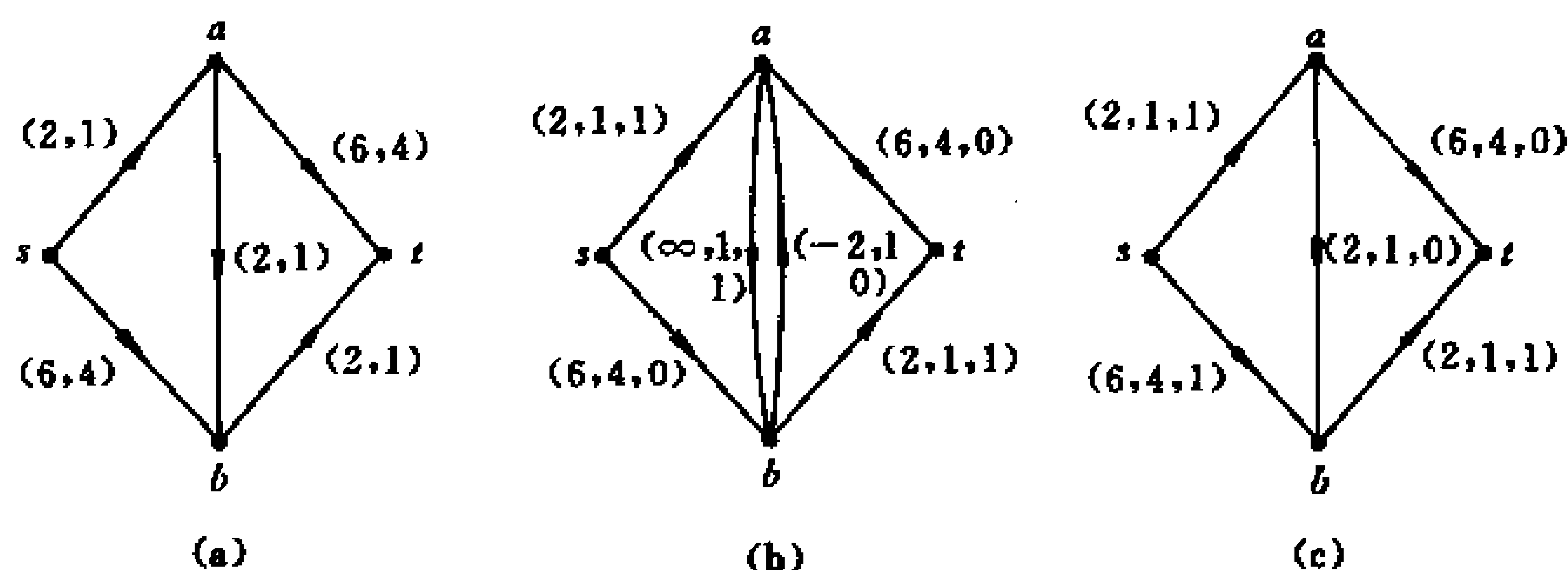


图 5.22

例 5.8.3 设 $w=2$，图 5.22(a) 中每边的两个权分别是 a_{ij}，和 c_{ij}，求它的最小费用流。

解：初始 $w_0=0$，各边的费用 $a_{ij}^*=a_{ij}$，$P=(s,a,b,t)$是当前的最短增流路，$\lambda_t=1$，故 $w_0=1$，容许流分布如 5.22(*b*)，每边的第 3 个权是当前的容许流分布。注意，当边 $(i,j)(i,j\neq s,t)$的 $f_{ij}>0$ 时，就对应存在一条边(j,i)，并且 $a_{ji}=-a_{ij}$，$c_{ji}=c_{ij}$，$f_{ji}=0$。这时再求 s 到 t 的最短增流路：$P=(s,b,a,t)$，$\lambda_t=1$，$w_0=2$，满足要求，因此最终的最小费用流分布如图 5.22(*c*)，最小费用是$\sum a_{ij}f_{ij}=16$。

最后再介绍一个多源多汇的最小费用流的例子。

例 5.8.4 已知网络流图 5.23，发点 a、b 均可供应两个单位，

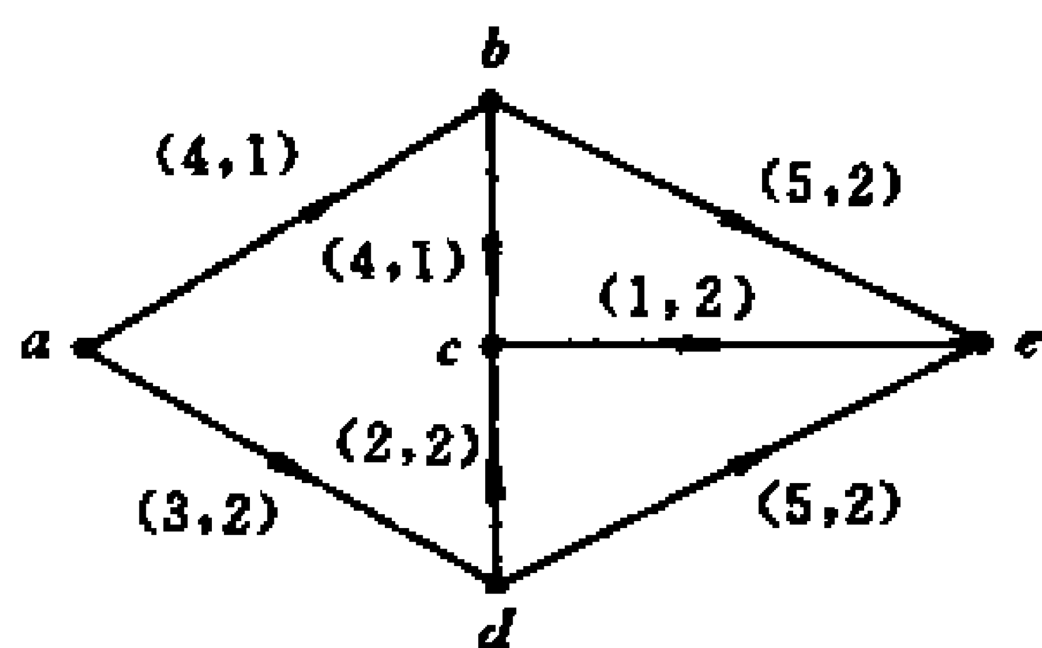
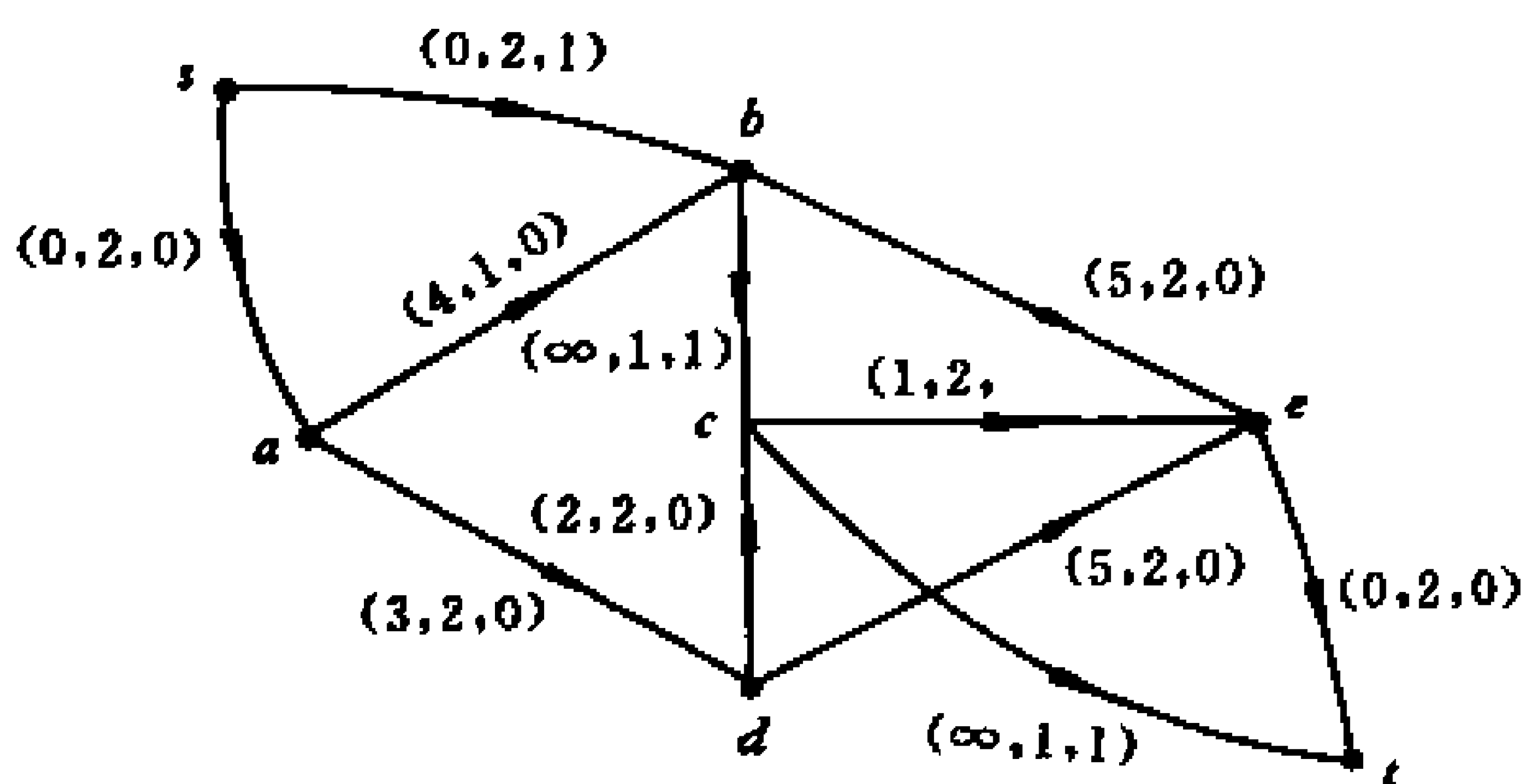


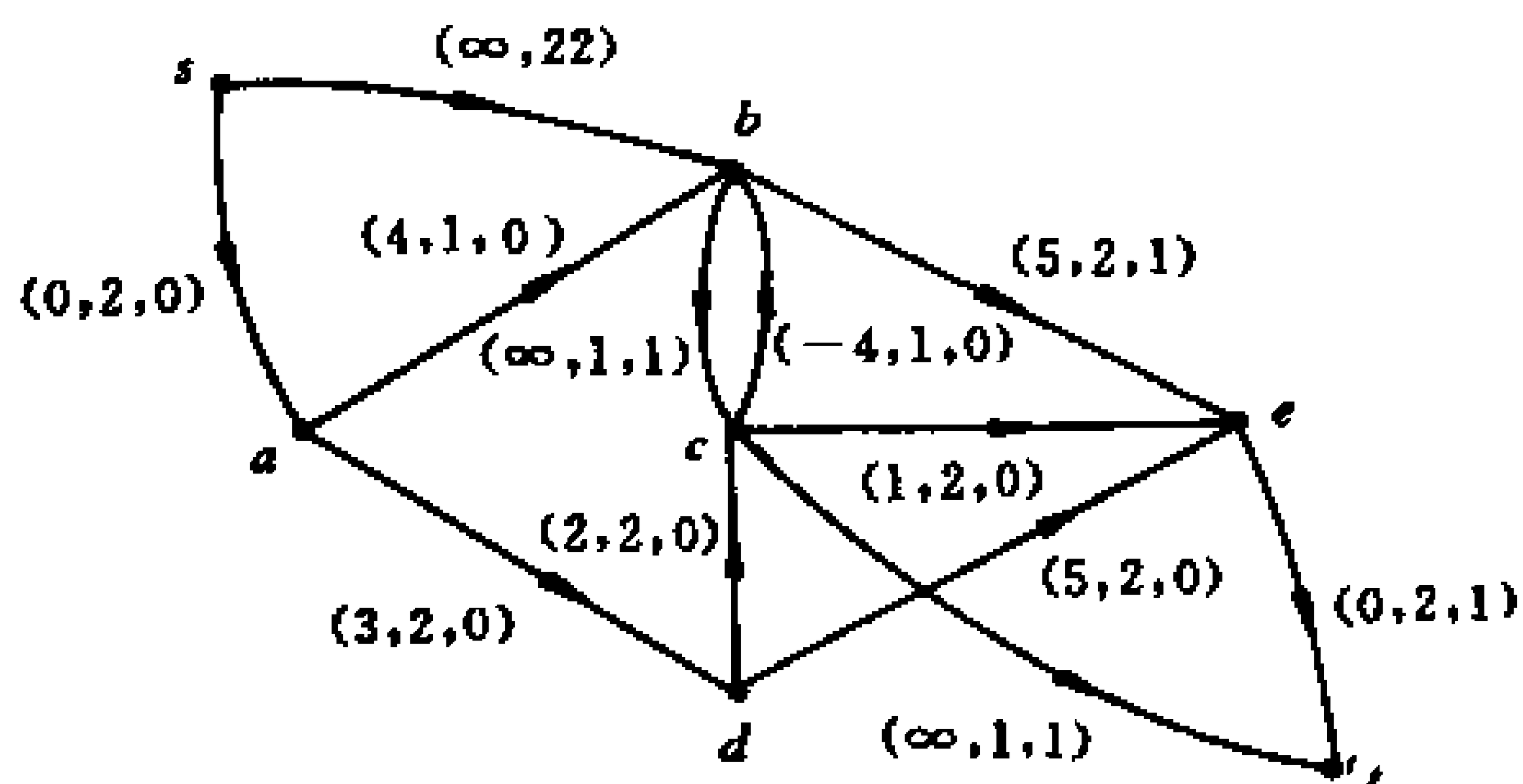
图 5.23

收点 c 接收 1，e 接收 2 个单位，求其最小费用流。

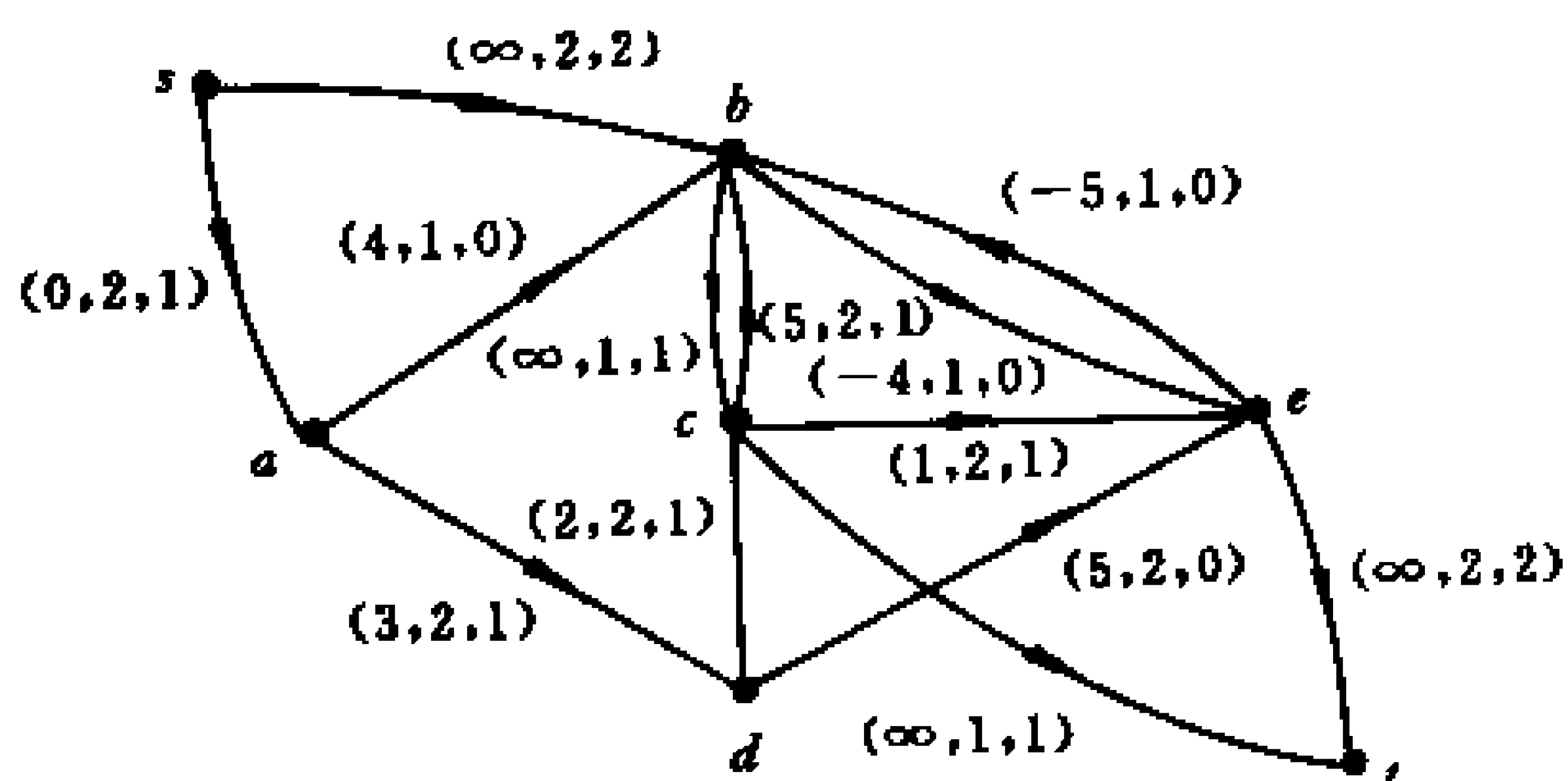
解：增设一个超发点 s，最初 $a_{sa}=0$，$c_{sa}=2$，$a_{sb}=0$，$c_{sb}=2$；增设一个超收点 t，初始 $a_{ct}=0$，$c_{ct}=1$，$a_{et}=0$，$c_{et}=2$。依次求出的最短增流路是 $P_1=(s,b,c,t)$，$\delta_t=1$；$w_0=1$；$P_2=(s,b,e,t)$，$\delta_t=1$，$w_0=2$；$P_3=(s,a,d,c,e)$，$\delta_t=1$。$w_0=3$，分别如图 5.24(a)，(b)，(c)最后的流分布如图 5.25，$\sum a_{ij}f_{ij}=15$。



(a)



(b)



(c)

图 5.24

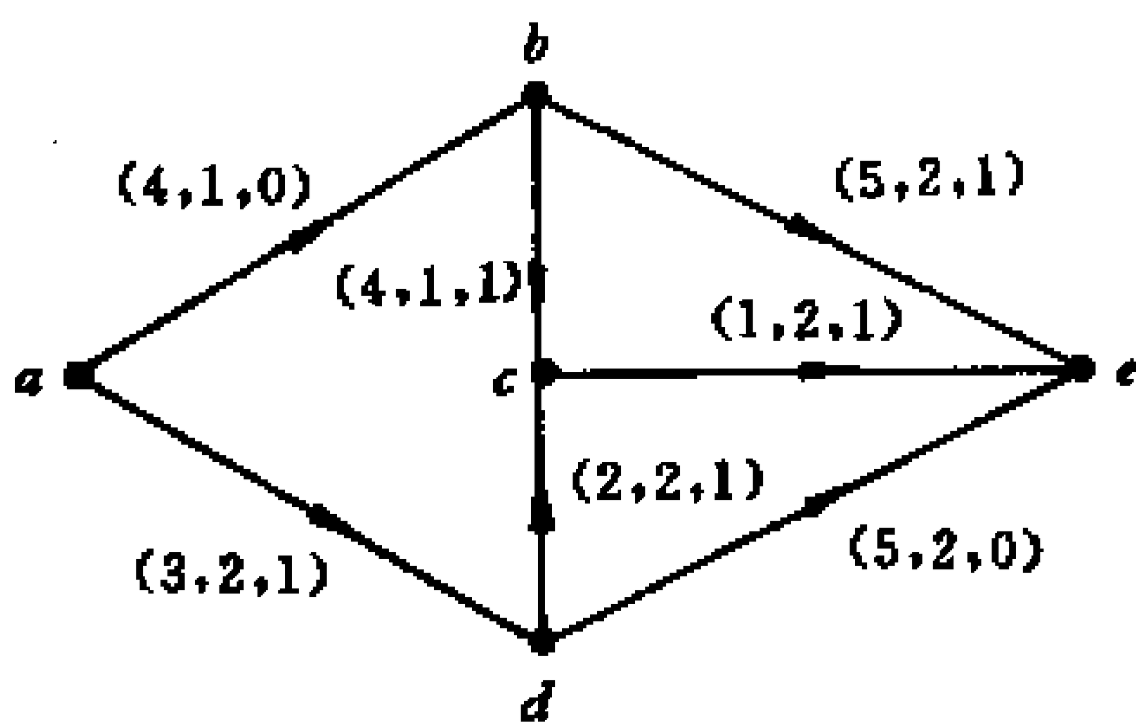
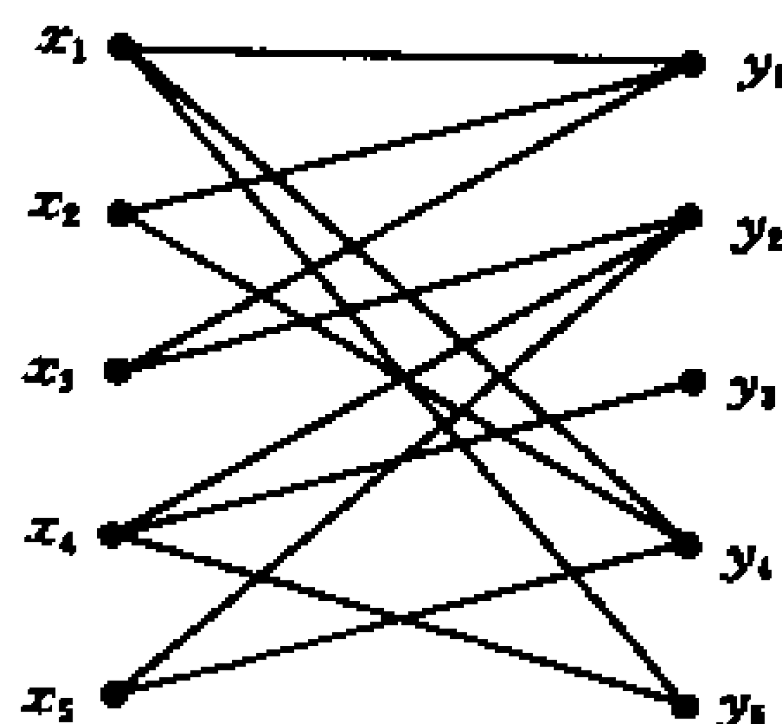


图 5.25

习 题 五

1. 已知二分图，初始匹配是 $M=\{(x_1,y_1),(x_4,y_2)\}$，求最大匹配。



题图 5.1

2. 有 5 个字符串 bc、ed，ac，bd 和 abe，能否用其中的一个字母代表该字符串并且不产生混淆？如果可以试给出一种方案。

3. 证明：$2n$ 个结点的树中最多只存在一个完全匹配。

4. 设图 G 的结点是由所有 0 和 1 的 k 元组所组成，且仅当两个 k 元组有一个坐标不同时，这两个结点相邻，这种图称为 k—方体图。证明：

(1) k—方体图是有 2^k 个结点 $k\cdot 2^{k-1}$条边的二分图。

(2) k—方体图存在完全匹配。

5. 证明定理 5.2.2。

6. 计算：

(1) k_{2n}中的不同的完全匹配数目。

(2) $k_{n,n}$中不同的完全匹配数目。

7. 由 0、1 元素组成的矩阵 A 每行都有 k 个 1 元素，每列 1 元素的数目不超过 k 个。问能否使 $A=P_1+P_2+\cdots+P_k$ 成立，其中 P_i ($i=1$, 2, …, k) 的每行都有一个 1 元素，每列最多只有一个 1 元素？

8. 6 位教师 y_1，…，y_6 给 4 个班 x_1，…，x_4 上课，课时安排由下表给出，c_{ij}表示教师 y_j 给班 x_i 每周上课的学时数。已知教室固定，问能否都安排在每天的前二节上课？试说明理由。

$$C=\begin{bmatrix}3 & 0 & 3 & 2 & 2 & 2\\ 2 & 3 & 2 & 3 & 2 & 0\\ 2 & 3 & 0 & 2 & 2 & 3\\ 0 & 2 & 3 & 2 & 3 & 2\end{bmatrix}$$

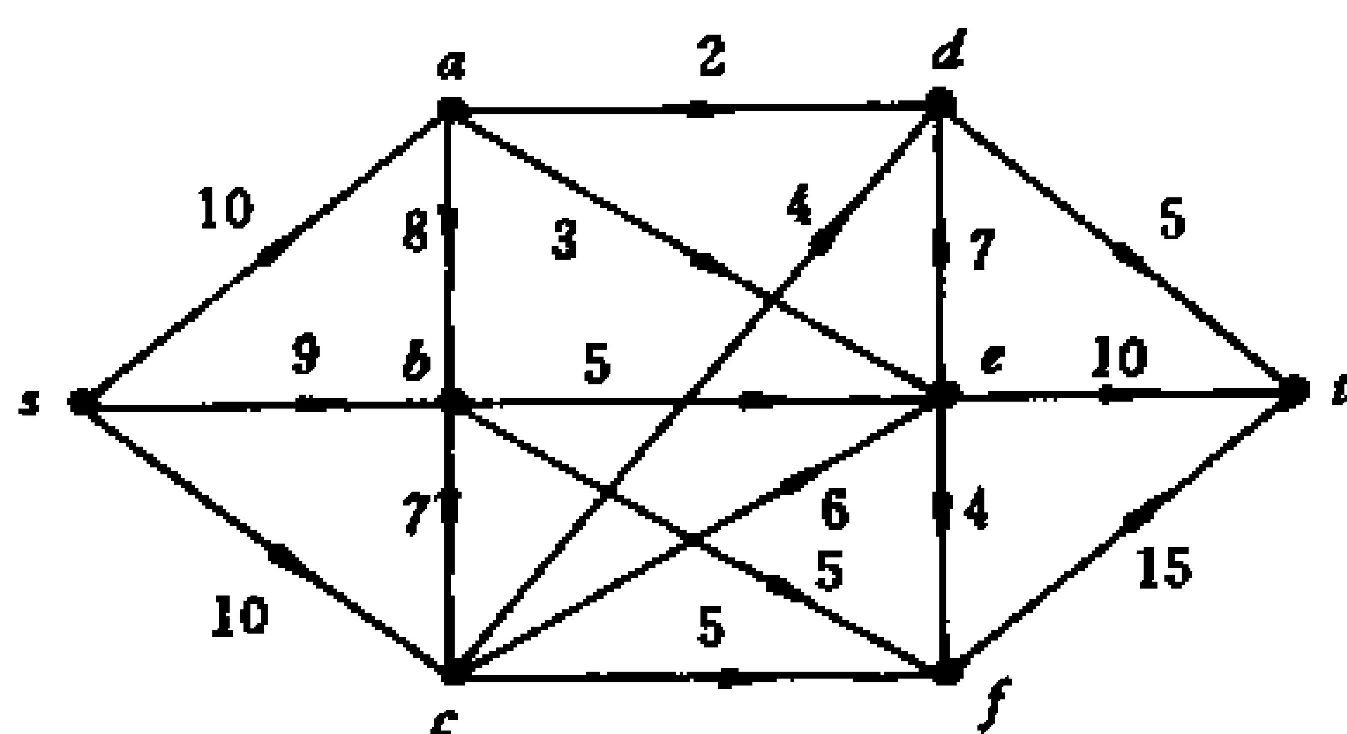
9. 已知利润矩阵，求最大利润。

$$\begin{bmatrix}5 & 4 & 5 & 3 & 5 & 8\\ 7 & 3 & 6 & 6 & 6 & 10\\ 5 & 6 & 8 & 4 & 2 & 9\\ 11 & 7 & 6 & 8 & 3 & 2\\ 8 & 9 & 5 & 4 & 6 & 7\\ 7 & 4 & 3 & 2 & 4 & 5\end{bmatrix}$$

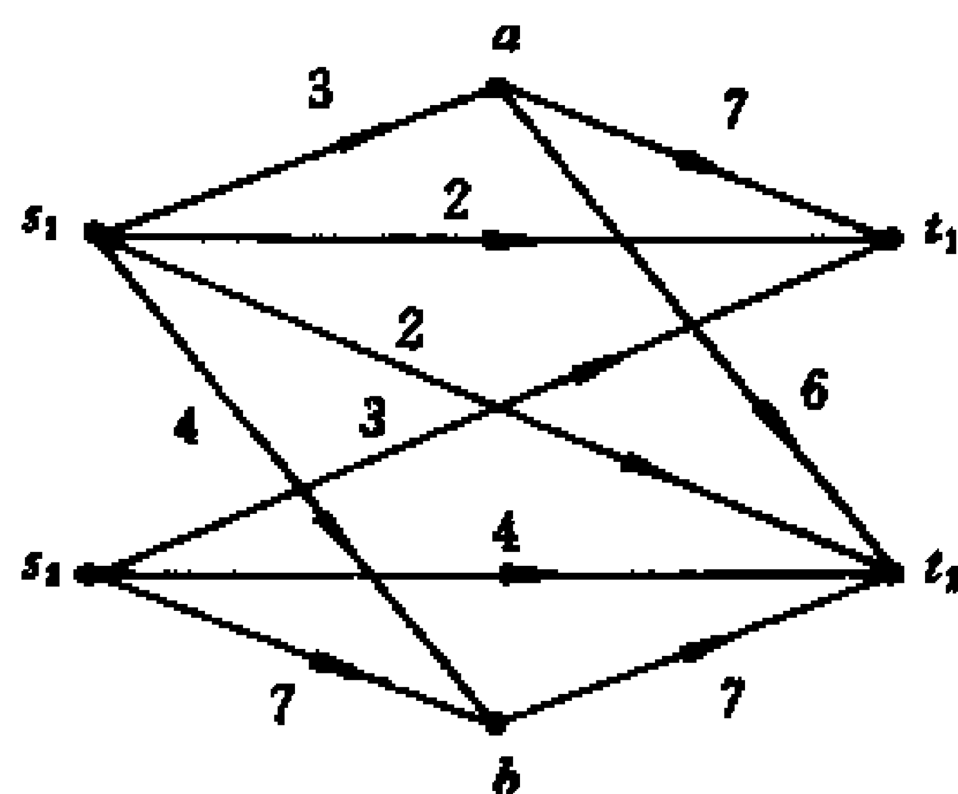
10. 若上表是成本矩阵，求它的最小成本。

11. 求图的最大流和最小割切。

12. 网络流图，发点 s_1，s_2 分别可供应 10 和 15 个单位；收点 t_1 和 t_2 可以接收 10 和 25 个单位，求最大流分布。



题图　5.11



题图　5.12

13. 对任意一个网络流图 N 增加一条边 e_u，并着以黑色，对 N 中其余边任意着以黑、红、绿三种颜色，证明以下两种情况之一必然出现：

(1) 存在一条由黑色或红色边构成的包含 e_u 的回路 C，C 中所有黑色边的方向一致。

(2) 存在一个包含 e_u 的由黑色或绿色边构成的边集 A，$G-A$ 分成二个结点集 V_1、V_2（设其中 $t\in V_1$），满足 A 中全部黑色边都是由 V_1 指向 V_2。

14. 由上题结论证明最大流最小割切定理。

15. 求图的最小费用流，设 $w_0=8$。

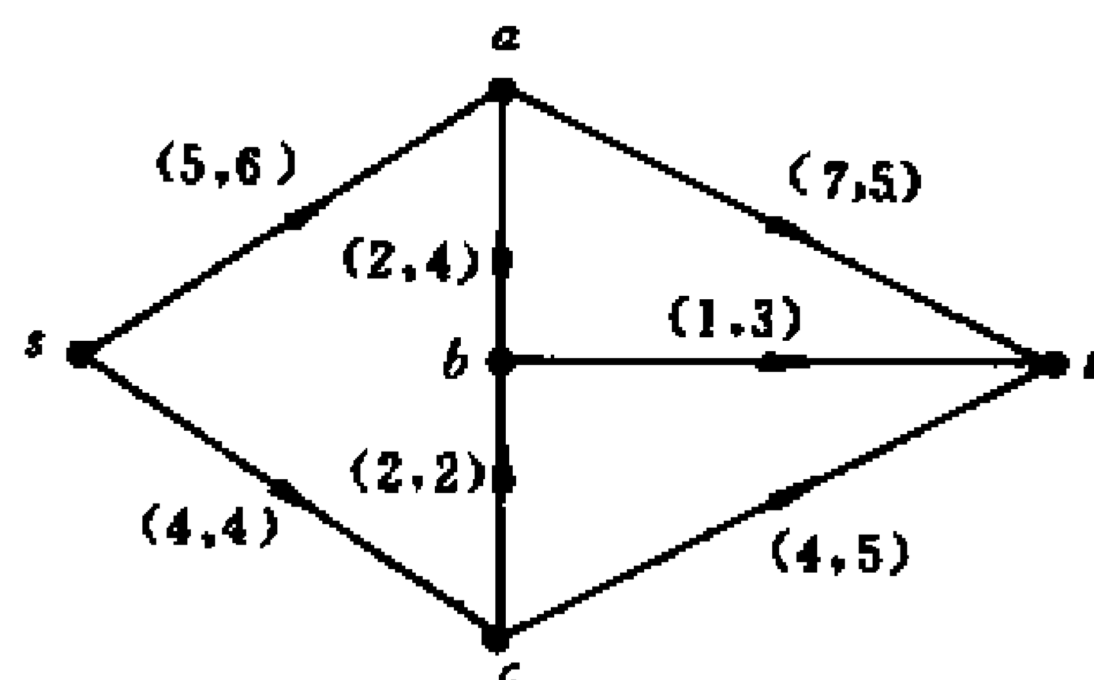
16. 编写计算二分图最大匹配的程序。

17. 编写计算二分图最佳匹配的程序。

18. 编写求最大基数匹配的程序。

19. 编写最大流算法程序。

20. 编写最小费用流算法的程序。



题图　5.15

第六章　图 的 连 通 性

6.1　割点、割边和块

我们已经知道，有些连通图移去了一条边或一个结点就变得不连通了。特别是树，移去任何一条边或任意一个非树叶结点就会不连通，具有这样性质的边和结点就是割边和割点。

定义 6.1.1　设 v 是 G 中的一个结点，如果 $G-v$ 的连通支数比 G 多，就称 v 是 G 的一个割点。

根据定义，如果 v 是连通图 G 的一割点，那么 $G-v$ 就是非连通图。

定义 6.1.2　图 G 最大的没有割点的连通子图称为块。

例 6.1.1　图 6.1（a）中 v 是割点，它有 3 个块，如（b）所示。注意 u 不是割点。

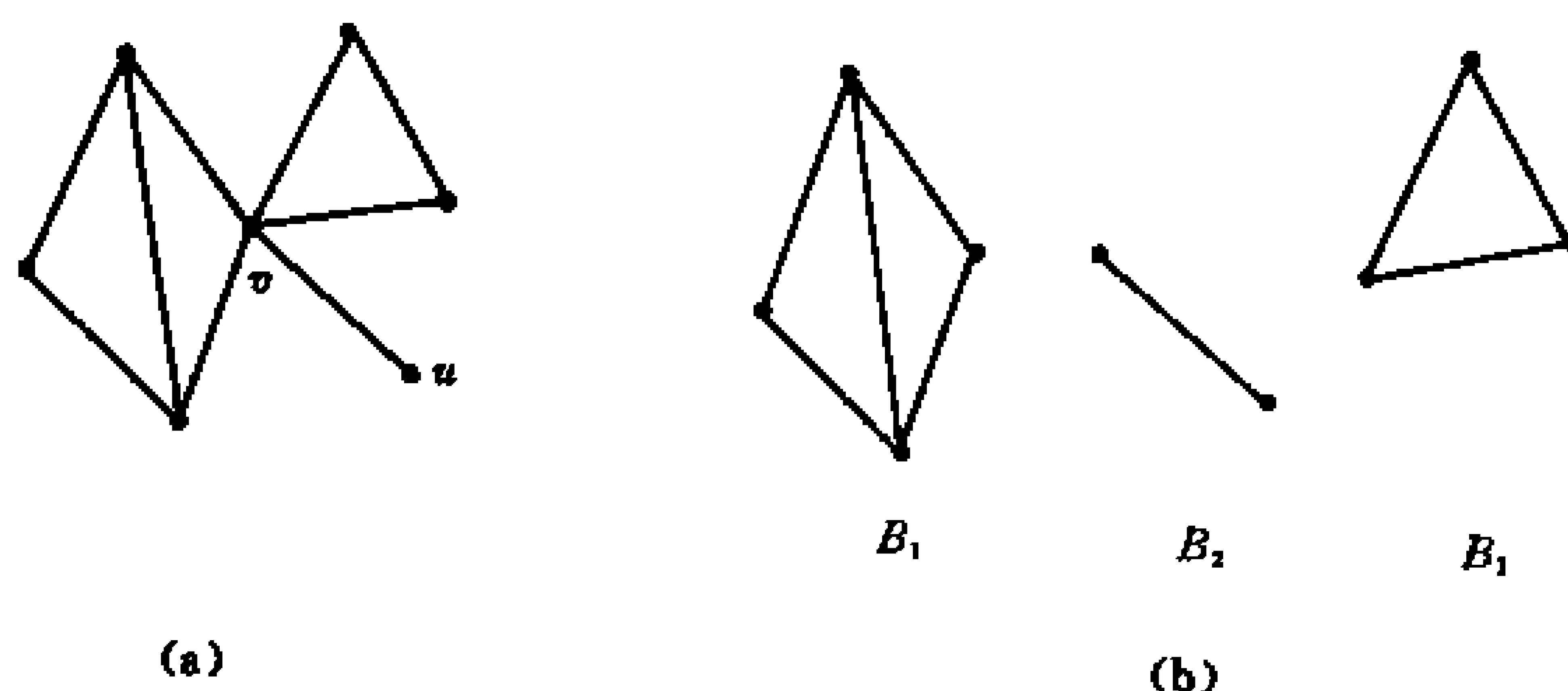


图　6.1

以下分别讨论它们的性质。

定理 6.1.1　设 v 是连通图 G 的一个结点，则下述性质等价：

1. v 是 G 的一个割点。

2. 存在与 v 不同的两个结点 u 和 w，使任一条 u 到 w 的道路 P_{uw} 都经过 v。

3. $V-v$ 可以划分为两个结点集 U 和 W，使对任意结点 $u\in U$ 和 $w\in W$，结点 v 都在每一条道路 P_{uw} 上。

证明：

1=>3　因为 v 是割点，$G-v$ 至少有两个连通支，设 U 是其中一个连通支的结点集，W 是其余结点集，因此 U 和 W 构成了 $V-v$ 的划分。由于任何两点 $u\in U$ 和 $w\in W$ 分别在 $V-v$ 的不同连通支中，所以 G 中每一条道路 P_{uw} 必过结点 v。

3=>2　2 是 3 的一个特例，显然成立。

2=>1　因为任一条道路 P_{uw} 都经过 v，所以 $V-v$ 中 u 和 w 之间将不存在道路，即 G 的连通支数增加，由定义 6.1.1，v 是 G 的割点。

定理 6.1.2 令 e 是连通图 G 的一条边，下述性质是等价的：

1. e 是 G 的一条割边。

2. e 不属于 G 的任何回路。

3. 存在 G 的结点 u 和 w，使 e 属于 u 和 w 的任何一条道路 P_{uw}。

4. $G-e$ 可以划分为两个结点集 U 和 W，使得对任何结点 $u\in U$ 和 $w\in W$，在 G 中道路 P_{uw}都经过 e。

证明：

1=≥4　因为 e 是割边，由定理 3.1.1，$G-e$ 划分成两个连通支，其结点集就是 U 和 W。所以连通图 G 的任意两点 $u\in U$ 和 $w\in W$，其道路 P_{uw}都经过 e。

4=＞3　在 $G-e$ 中，U 和 W 都不是空集。结论得证。

3=＞2　由于 u 和 w 之间不存在不经过 e 的任何道路，因此 $P_{uw}+e$ 不可能构成回路。

2=＞1　如果 $e=$（u，w）不是割边，则 $G-e$ 中 u 和 w 之间仍存在一条道路 P_{uw}，$P_{uw}+e$ 便构成了一个包含 e 的回路。

定理 6.1.3 设 G 是至少有 3 个结点的连通图，则下述性质等价：

1. G 是一个块。

2. G 的任何两结点同属某一初级回路。

3. G 的任何一个结点和任何一条边同属于某个初级回路。

4. G 的任何两条边同属某一初级回路。

5. 给定两个结点 u、v 和一条边 e，存在一条包含 e 的道路 P_{uv}。

6. 对 G 的任意三个不同的结点，存在一条包含它们的初级道路。

7. 对 G 的任意三个不同的结点，存在一条只含其中两点而不含第三点的道路。

证明思路如下：

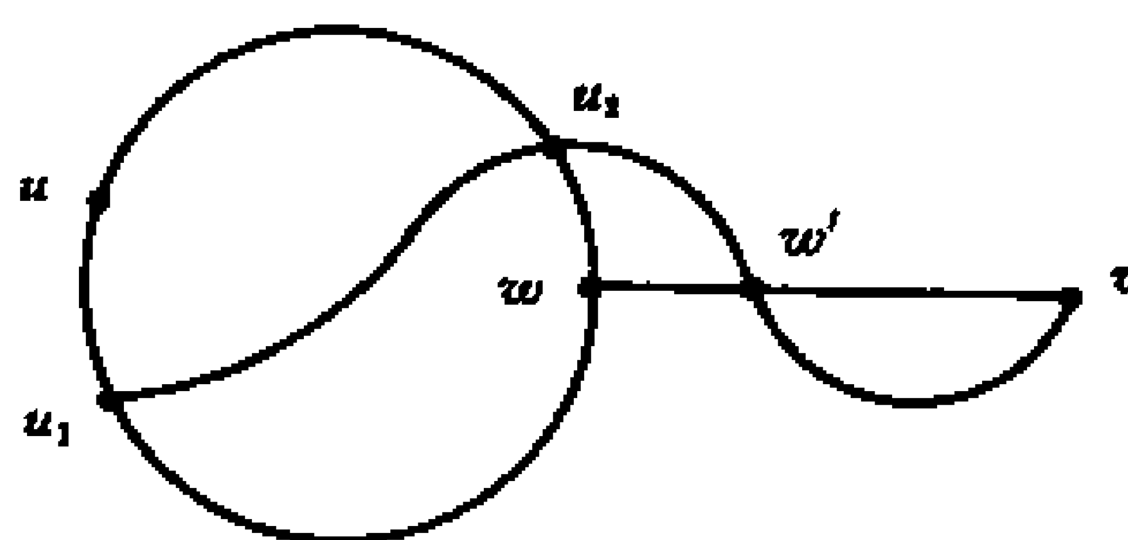


图　6.2

1=＞2　令 u，v 是 G 中不同的结点，U 是 G 中能与 u 同属某一初级回路的结点集合，若 $U=V$ 即得证。假定 $v\notin U$，设 C 是在全部含 u 的初级回路 C' 里，使 P_{wv}（$w\in C'$）为最短的一个回路，如图 6.2 所示。因为 G 是块，故 w 不是割点，uv 之间存在另一条道路 $P'=P_{uu_1}+P_{u_1u_2}+P_{u_2w'}+P_{w'v}$。如果 P' 不与 P_{wv}相交，易知 u 与 v 同在某个初级回路上。若存在这样的交点 w'，又易见 w' 与 u 同在某个初级回路上，但此时 $P_{w'v}$比 P_{wv}更短。与 w 的选择矛盾。

2=＞3　设 u 和（v，w）是 G 中任一结点和边，u 和 v 在 G 的某一初级回路 C 上，若（v，w）$\in C$，命题成立。否则，因为 u 和 w 也在某一初级回路 C' 上，u 是 C 和 C' 的公共点，（v，w）是两端点分别在 C 和 C' 上的一条边，各自选择 C 和 C' 上的一条道路 P_{uv} 和 P_{uw}，加上边（v，w）便可构成一个初级回路。

3=＞4　与上述证明类似。

4=＞5　由 4，显见任何两个结点同属某一回路，即得 2，由 2=＞3，设 u，v 和 $e=$

(x, y) 是任给的结点和边，则 u，e，v，e 分别在同一初级回路 C_1 和 C_2 上。$e \in C_1 \cap C_2$。不管 u，v 如何相处，此时一定存在经过 e 的道路 P_{uv}。

5=>6　令 u，v，w 是 G 中三个不同的结点，e 是与 w 关联的一条边，则 G 中存在包含 e 的道路 P_{uv}，即 w 在 P_{uv} 之中。

6=>7　由 6，G 中存在包含 v 的道路 P_{uw}，显然其中的道路 P_{uv} 不包含 w。

7=>1　因此，舍弃 G 中任何一个结点 w，任意两个结点之间在 $G-w$ 中仍存在道路，所以 G 中没有割点，亦即它是一个块。

6.2　结点与边的连通度

图的连通度推广了割点、割边的概念。一个连通图 G 可能没有割点和割边，但当移去若干个结点或若干条边之后，它就成为不连通的了。这些结点和边的集合就叫点断集和边断集。

定义 6.2.1　连通图 G 在移去若干结点之后至少分为两个连通子图或剩下一个孤立点，则这些结点的集合称为 G 的一个点断集或断集，记为 A。
并称

$$\kappa(G) = \min_{A \in \phi}\{|A|\}$$

为断量。其中 ϕ 是断集集合。

定义 6.2.2　如果连通图 G 移去若干条边之后变为非连通的，则这些边的集合称为 G 的一个边断集，记为 B。并称

$$\lambda(G) = \min_{B \in \psi}\{|B|\}$$

为边断量，其中 ψ 是边断集集合。

显然，若 $\kappa(G)=1$，G 中有断点；$\lambda(G)=1$，G 中有割边。对于完全图 K_n 来说，$\kappa(G)=\lambda(G)=n-1$。

定理 6.2.1　连通图 G 中，有

$$\kappa(G) \leqslant \lambda(G) \leqslant \delta(G),$$

其中 $\delta(G)$ 是结点的最小度。

证明：设 v 是 G 中具有最小度的结点，显然删去与 v 关联的这 $\delta(G)$ 条边之后，G 将成为非连通图。因此 $\lambda(G) \leqslant \delta(G)$。以下再证 $\kappa(G) \leqslant \lambda(G)$。设 $B=\{e_1, e_2, \cdots, e_\lambda\}$ 是 G 的一最小边断集，$G-B$ 至少有两个不连通的结点集 V_1，V_2。这时在 G 的结点子集 V_1 中删去与 e_1，e_2，$\cdots$，$e_{\lambda-1}$ 相关联的最多 $\lambda-1$ 个结点，并在 V_2 中删去与 e_λ 相关联的一个结点之后，G 将不连通，亦即这些结点的集合 A 便构成了 G 的一个断集。因此 $\kappa(G) \leqslant \lambda(G)$。

定义 6.2.3　G 是连通图，任给 $k \geqslant 1$，当 $\kappa(G) \geqslant k$ 时，称 G 是 k 连通图。$\lambda(G) \geqslant k$ 时，称为 k 边连通图。

例如树 T 是 1—连通图，也是 1—边连通的。初级回路 C 是 1—连通的，也是 2—连通图。至少有 3 个结点的块既是 2—连通的，也是 2—边连通的。

定理 6.2.2 简单连通图 G 中有

$$\kappa(G) \leqslant \left\lfloor \frac{2m}{n} \right\rfloor。$$

证明： $\because \quad \sum d(v_i) = 2m$，

$\therefore \quad n\delta(G) \leqslant 2m$，

$$\delta(G) \leqslant \left\lfloor \frac{2m}{n} \right\rfloor。$$

再由定理 6.2.1 即得证。

该定理说明，对一个简单 k 连通图，如果令 $f(k, n)$ 表示其边的数目，不等式 $f(k, n) \geqslant \left\lceil \frac{kn}{2} \right\rceil$ 就会成立。

那么是否存在一个 k 连通图能恰好满足 $f(k, n) = \left\lceil \frac{kn}{2} \right\rceil$ 呢？哈拉里（Hararry）构造了这类的图，并证明了它们满足上述条件。

哈拉里的构造方法如下，分三种情形：

1. $k=2r$。

设 $G_{2r,n}$ 的结点为 v_0，v_1，…，v_{n-1}，若 $i-j \leqslant r \pmod n$ 则 $(v_i, v_j) \in E$。

2. $k=2r+1$，且 $n=2l$。

若 $i-j \leqslant r \pmod n$，则 $(v_i, v_j) \in E$。

若 $i-j=l \pmod n$，则 $(v_i, v_j) \in E$。

3. $k=2r+1$ 且 $n=2l+1$.

若 $i-j \leqslant r \pmod n$，则 $(v_i, v_j) \in E$.

若 $i-j=l+1 \pmod n$，则 $(v_i, v_j) \in E$。

对剩下的一点 v_t，令 v_t 与满足 $t-j=l \pmod n$ 的某点 v_j 相邻。

例 6.2.1 由哈拉里的方法构造的一些图如图 6.3。

定理 6.2.3 由哈拉里的方法构造的 $G_{k,n}$ 是 k 连通的。

证明：只需证明 $\kappa(G)=\delta(G)$。令 n 个结点分别是 0，1，…，$n-1$，假定 V' 是一个断集，满足 $|V'|<\delta(G)$，设 i，j 分属于 $G-V'$ 的两个不同的连通支，这时 G 的 n 个结点可分成两部分

$$S=\{i, i+1, \cdots, j-1, j\} \qquad \pmod n。$$
$$T=\{j, j+1, \cdots, i-1, i\} \qquad \pmod n$$

仍按三种构造情况讨论。

(1) 设 $\delta(G)=2r$，由于 $|V'|<2r$，i，$j \notin V'$，根据抽屉原理，$|V' \cap S|$ 或 $|V' \cap T|$ 中一定有一个小于 r，不妨令 $|V' \cap S|<r$，这样 S 中不可能有连续的 r 个结点属于 V'，换言之，$S-V'$ 里一定有若干个点 $i, i_1, i_2, \cdots, i_k, j$，满足 $(i-i_1), \cdots, (i_k-j) \leqslant r \pmod n$，亦即存在 i 到 j 的道路 $(i, i_1, \cdots, i_k, j)$，与 i，j 在不同的连通支矛盾。

(2) 设 $\delta(G)=2r+1$，$n=2l$。

若 $|V'|<2r$，证法同(1)，现设 $|V'|=2r$。若 $|V' \cap S| \neq |V' \cap T|$，则其中一个比如 $|V' \cap S| \leqslant r-1$，如(1)可证。若 $|V' \cap S|=|V' \cap T|=r$，由于 $\delta(G)<n-1$，所以 $r \leqslant \frac{n-2}{2}=l-$

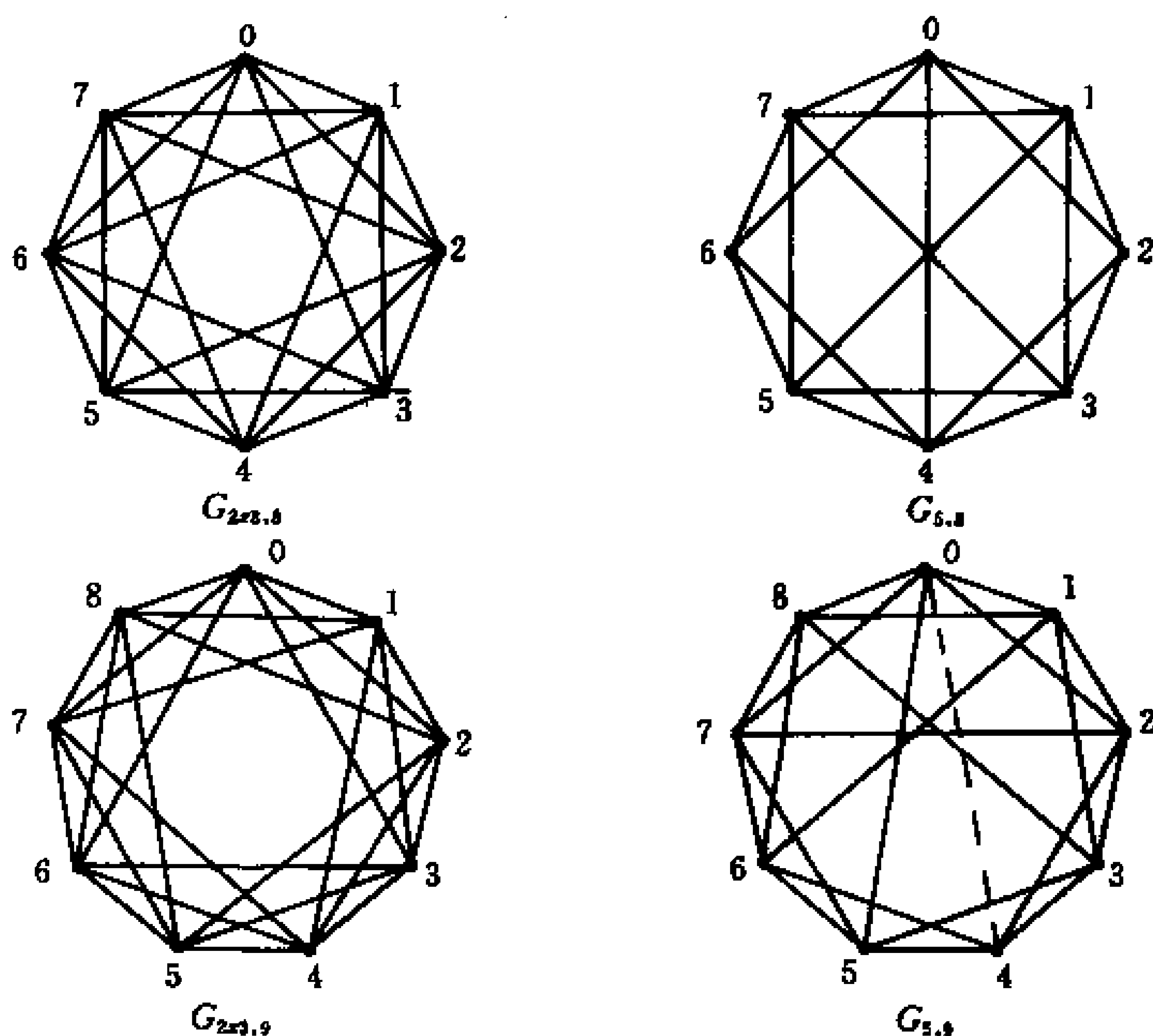


图 6.3

1，又因为 i、j 不可能是对角线的两端点，所以 S 或 T 中至少有一个所含结点数大于 $l+1$，设 $|S|\geqslant l+2$，故有 $|S-V'|>2$，类似(1)可证 S 中有 i 到 j 的道路，矛盾。

(3)类似(2)可证。

综上说明当 $|V'|<\delta(G)$ 时，V' 不可能是断集，故 $\kappa(G)=\delta(G)$。

以下讨论两个关于连通度的存在性定理。

定理 6.2.4 设 G 是 n 个结点的简单图，假定 G 的结点度排序满足 $d(v_1)\leqslant d(v_2)\leqslant\cdots\leqslant d(v_n)$，且

$$d(v_r)\geqslant r+k-1,\qquad 1\leqslant r\leqslant n-1-d(v_{n-k+1})。$$

则 G 是 k 连通的。

证明：令 G 满足定理条件但不是 k 连通的，则存在一断集 S，满足 $|S|=s<k$ 并使 $G-S$ 成为不连通。令 H（$|H|=h$）是其中结点数最少的一个支，H 中每个结点的度 $d(v_k)\leqslant h-1$，因此在 G 里 H 中的结点最大度不超过 $h+s-1$，即

$$d(v_h)\leqslant h+s-1<h+k-1,$$

这不满足定理条件，所以

$$h>n-1-d(v_{n-k+1})。\tag{1}$$

由于 $G-S$ 有 $n-s$ 个结点，且 H 是 $G-S$ 中结点数最少的一个支，故有

$$h\leqslant n-s-h\quad 或\quad h+s\leqslant n-h,$$

也就是说在 G 中，H 的结点 v 有

$$d(v)\leqslant h+s-1\leqslant n-h-1。$$

由于 $V(G)-V(H)-S$ 里的结点在 G 中最多与 $n-h-1$ 个结点相邻，所以 $V-S$ 的任一

点 V_{n-s}都有

$$d(v_{n-s}) \leqslant n-h-1。$$

由 (1)

$$d(v_{n-s}) < d(v_{n-k+1}),$$

即

$$n-s < n-k+1。$$

或

$$s \geqslant k。$$

与假设矛盾。

图 6.4

例 6.2.2 当 $k=3$ 时，图 6.4 满足定理 6.2.4 的条件。因此它是 3－连通的。

关于边连通度的一个充分性定理如下

定理 6.2.5 设 G 是 n 个结点的简单图，若

$$\delta(G) \geqslant \left\lfloor \frac{n}{2} \right\rfloor, 则\ \lambda(G) = \delta(G)。$$

证明：此时 G 一定是连通的？否则每个支至少有$\left\lfloor \frac{n}{2} \right\rfloor+1$ 个结点，与 G 只有 n 个结点矛盾。

现证 $\lambda(G)=\delta(G)$。假定 $\lambda(G)<\delta(G)$，则存在一个边断集 $S=(V_1,V_2)$，满足 $\lambda(G)=|S|<\delta(G)$。设 S 中的边与 V_1 的 p 个结点、V_2 的 q 个结点相关联，显然 $p,q\leqslant\lambda(G)$。设由 V_1 构成的 G 的导出子图是 G_1，则其边数

$$m_1 \geqslant \frac{1}{2}(p\delta(G)-\lambda(G))。$$

由于 $\lambda(G)<\delta(G)$，故

$$m_1 > \frac{1}{2}\delta(G)(p-1) > \frac{1}{2}p(p-1),$$

所以 $|V_1|>p$，同理 $|V_2|>q$。这说明 V_1 和 V_2 中都存在只与本子集内的结点相邻的点，因此

$$|V| = |V_1| + |V_2| \geqslant 2(\delta(G)+1),$$

与已知 $2\delta(G)+2>n$，矛盾。

例 6.2.3 图 6.5 满足定理 6.2.5 的条件，因此它是 3－边连通的

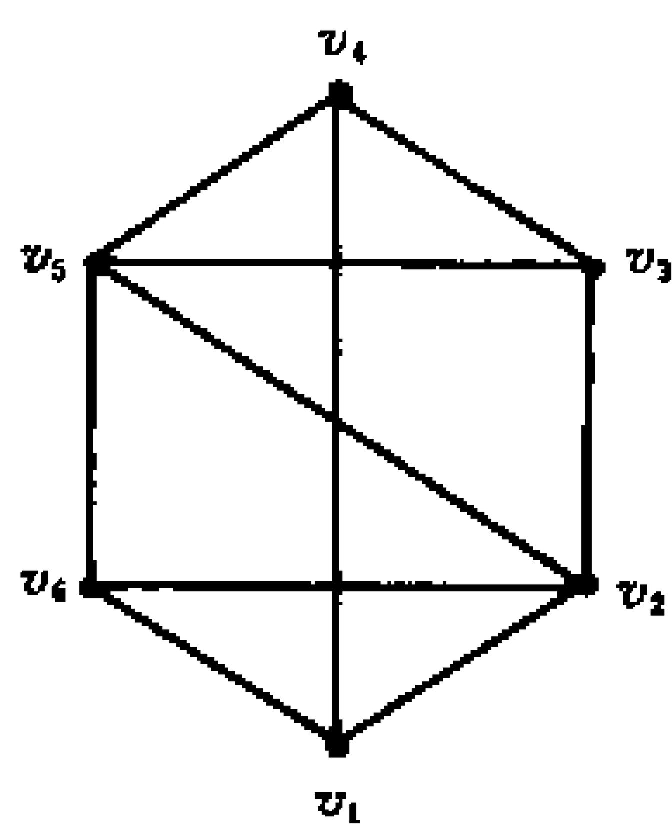


图 6.5

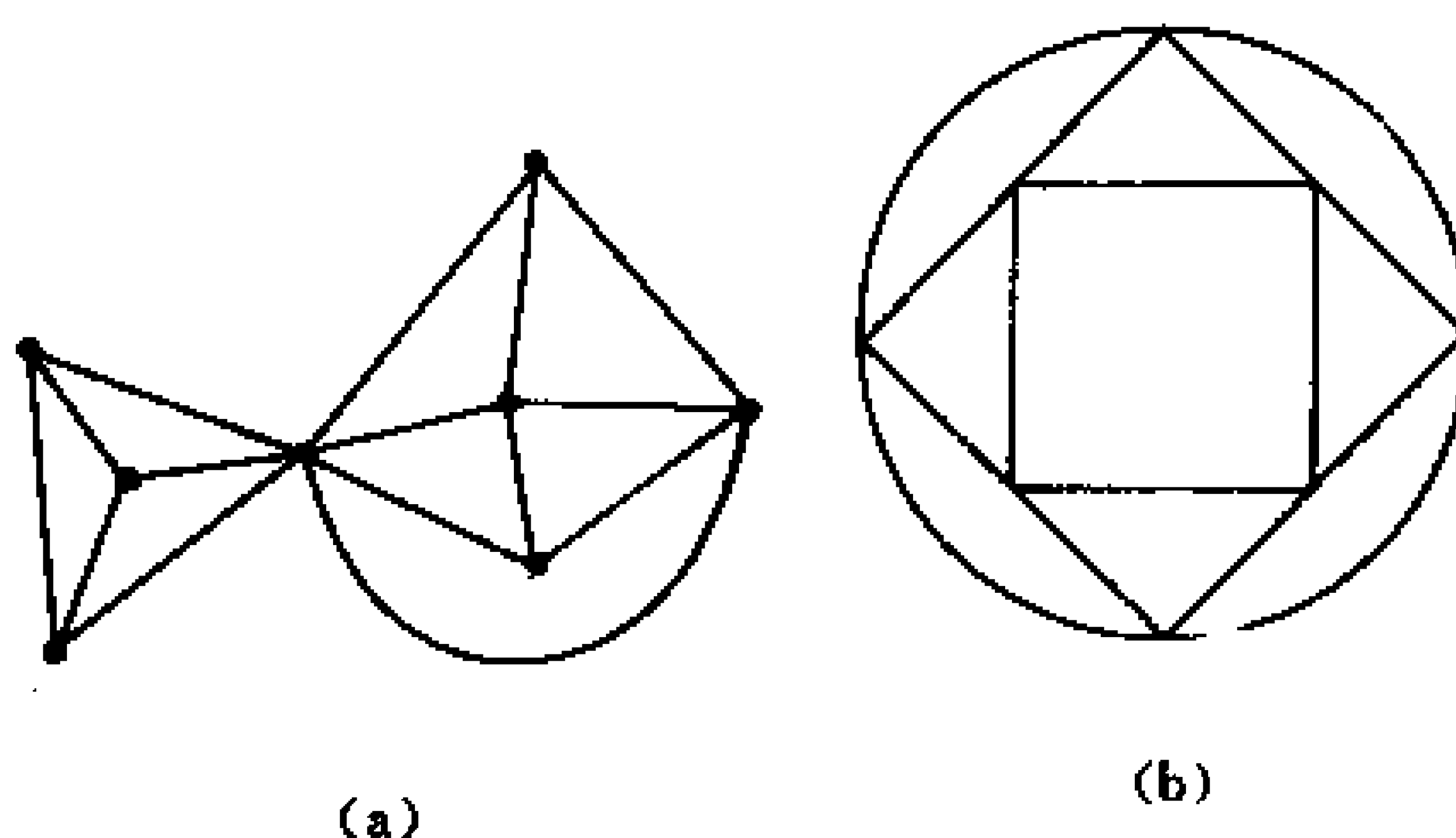


图 6.6

例 6.2.4 8 个输油站之间要修建 16 条输油管道，这时图 6.6(a)，(b)两个方案中显

然(b)的连通性能强。因为(a)中存在割点，且是3—边连通的，而(b)的点、边连通度都是4。

6.3 明格尔定理

明格尔(Menger)最先揭示了图的连通度与结点之间不相交道路数目的关系。

定义 6.3.1 设u，v是连通图G的两个结点，如果u和v之间的两条道路没有公共结点，称它们是不相交的道路；如果没有公共边，就说是边不相交的道路。

例如图 6.7 中，$P_1=(e_1,e_4,e_8)$和$P_2=(e_2,e_6,e_9)$是不相交的道路；$p_1'=(e_1,e_5,e_9)$和$P_2'=(e_2,e_3,e_4,e_8)$是边不相交的。

定理 6.3.1 分离两个不相邻结点s和t的最少结点数等于不相交的$s-t$道路的最多数目。

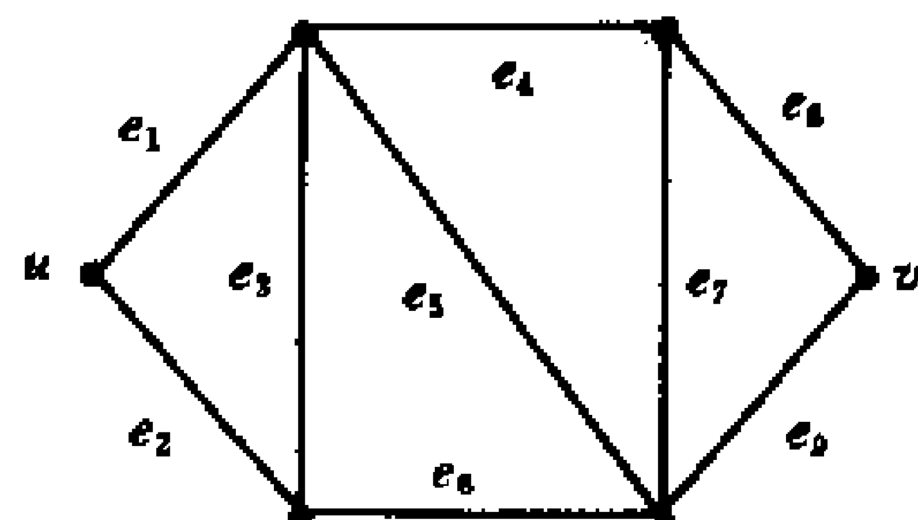


图 6.7

证明：设分离s和t的最少结点数为k，不相交的$s-t$道路的最多数目为l。因为每条道路上至少要移去一个结点才可能分离s和t，所以$k\geq l$，以下再证$k=l$。

当$k=1$时，结论成立。假定对某个$k>1$时不成立，令h是使等式不成立的最小k值，并设H是此时包含结点数最少的一个图，同时在H中移去某些边，直至得到G，使得在G中分离s和t需要h个结点，而且对G中的任意边e，在$G-e$中分离s、t只要$h-1$个结点。

这时，对任意$e\in E(G)$，$G-e$存在分离s，t的$h-1$个结点的断集$S(e)$，由于G中分离s，t需要h个结点，因此在$G-S(e)$中至少存在一条$s-t$道路，而且每条这样的道路一定经过边$e=(u,v)$，显然$u,v\notin S(e)$，且若$u\neq s,t$，则$S(e)+u$在G中分离s，t。于是我们可以得到两个结论：

1. G中不存在与s和t都相邻的点w，否则，令$e=(w,t)$，在$G-e$中分离s，t需$h-1$个结点且有$h-1$条不相交路，而$G-S(e)$中只有唯一道路(s,w,t)，因此G中一定只有h条不相交的$s-t$道路，与$k>l$矛盾。

2. 任何分离s和t的h个结点的断集W，若非每个结点都与s相邻，则一定都与t相邻。

在G中任给一个断集W，满足$|W|=h$，定义一条$s-W$的道路为$s-w_i$，$w_i\in W$，且不含W中其它结点。设所有$s-W$的道路集合为P_s，同理，设所有t到W的道路集合为P_t。这样每条$s-t$道路都是以P_s中的一条道路开始，P_t中的一条道路结束。当然其中一定含有W中的结点，而且每个结点w_i至少在P_s或P_t的一条道路之中。这时必有$P_s-W=\{s\}$或者$P_t-W=\{t\}$。否则，假定$P_t-W\neq\{t\}$，可以移去所有的w_i-t道路，并加入相应边(w_1,t)，(w_2,t)，…，得到图G'，在G'中分离s，t仍需h个结点，但它比G的结点数更少，与G的构造矛盾。

最后证明上述两个结论相悖。设$P=\{s, u_1, u_2, \cdots, t\}$是$G$中一条最短的$s-t$道路。令$(u_1,u_2)=e$，$S(e)=\{v_1,v_2,\cdots,v_{h-1}\}$在$G-e$中分离$s$和$t$。由结论1，$(u_1,t)\notin G$，亦

即 $u_2 \neq t$，令 $W=S(e)+u_1$，因为$(s,u_1)\in G$，所以根据结论 2，对一切 i 都有$(s,v_i)\in G$，而$(v_i,t)\notin G$。同理 $S(e)+u_2$ 也是 G 的一个断集 W'，由结论 2，因为断集 W' 中每个结点 v_i 都与 s 相邻，所以又有$(s,u_2)\in G$，但这与所选 P 是最短 $s-t$ 道路矛盾。定理得证。

例6.3.1 图 6.8 中，s 和 t 是不相邻的结点，移去 3 个点就可以分离它们，但不能再少，由定理 6.3.1，G 中不相交的 $s-t$ 道路最多有 3 条。

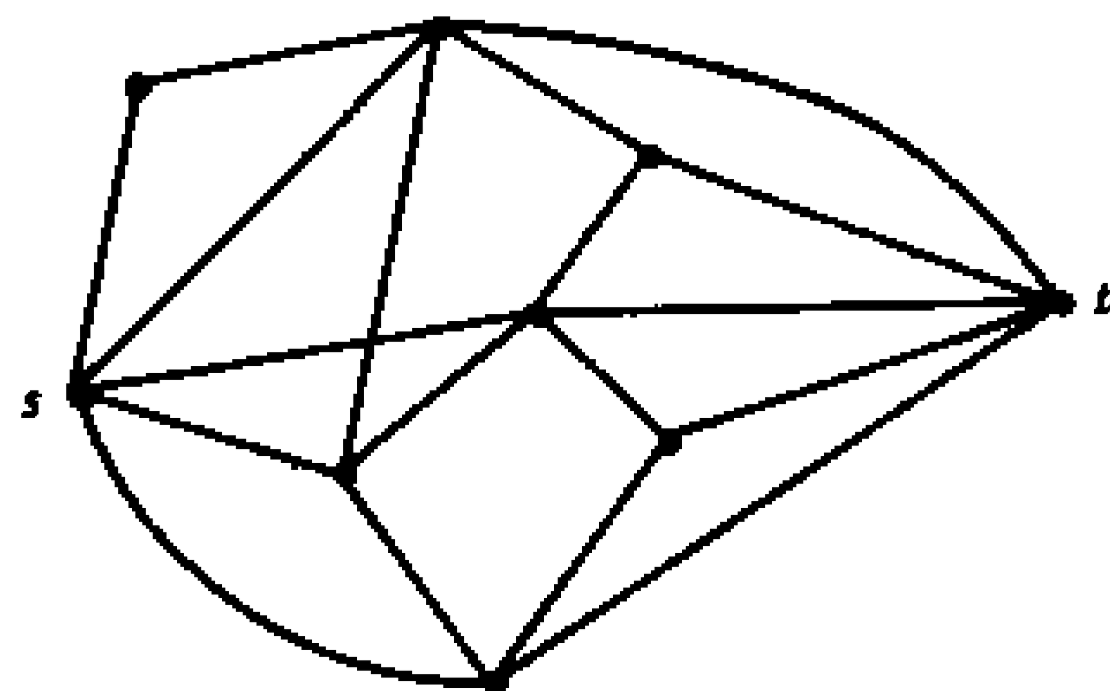


图 6.8

明格尔定理更一般的形式是：

定理 6.3.2 设 G 的结点数 $n\geqslant k+1$，G 是 k 连通的充要条件是 G 中任意两个结点 s 和 t 之间存在 k 条不相交的道路。

证明：$k=1$ 时显然，以下证 $k\geqslant 2$ 的情形。

必要性。若 s，t 不相邻，由定理 6.3.1 即得。假定 s，t 相邻且最多有 $k-1$ 条不相交的 $s-t$ 路，令 $e=(s,t)$，作 $G'=G-e$，则 G' 中最多有 $k-2$ 条不相交 $s-t$ 路。因此 G' 中存在一断集 $A\subseteq V-\{s,t\}$，满足 $|A|\leqslant k-2$，移去 A 即可分离 s 和 t，这时 $|V-A|=|V|-|A|\geqslant k+1-(k-2)=3$，因此 $V-A$ 中存在除 s 和 t 之外的结点 u。

以下证明 G' 中存在不经过 A 中结点的 $s-t$ 道路，即 A 并不是 G' 的断集。先证存在不过 A 的$s-u$道路。若$(s,u)\in G$ 立得，否则由定理 6.3.1，因为 G 是 k 连通的，所以 G 中存在 k 条不相交的 $s-u$ 道路，G' 中至少有 $k-1$ 条。由于 $|A|\leqslant k-2$，因此 G' 中至少有一条 $s-u$ 道路不过 A 的任何结点。同理 G' 中存在不过 A 的 $u-t$ 道路。因此 A 不是 G' 中分离 s 和 t 的断集，矛盾。

充分性。显然 G 连通，由于 G 不存在重边，因此最多有一条长为 1 的 $s-t$ 道路，其余 $k-1$ 条 $s-t$ 道路的同时至少含有 $k-1$ 个不同的结点 v_i，$v_i\neq s$，t，因此 $|V|\geqslant(k-1)+2>k$。

假定 G 中有一断集 A，$|A|<k$，考虑导出子图 G'，其结点集是 $V-A$。G' 中至少有两个连通支 G_1，G_2，在 G_1，G_2 中各选一个结点 s，t。这样 G 中最多只有 $|A|<k$ 条不相交的 $s-t$ 路。矛盾。

6.4 连通度的判定

上节讨论了结点的连通度与 G 中不相交道路之间的关系。类似地，关于边连通性也有以下两个定理。

定理 6.4.1 设 s，t 是无向图 G 的任意两个结点，则分离 s 和 t 的最少边数等于边不相交的 $s-t$ 道路的最多数目。

证明：我们利用网络最大流的方法来证明。首先根据图 G 构造相应网络 N 如下：N 包含了 G 的所有结点；对 G 中的每条边(u,v)，N 中对应两条有向边(u,v)和(v,u)，且对每条边 $e\in N$，令其容量 $C(e)=1$。这样对 N 中的任一容许流分布 f，都有 $f(e)=0$ 或 1，我们设 N 中从源 s 到汇 t 的最大流为 F。同时为方便起见，令 G 中分离 s 和 t 的最少边数

为 $c_e(s,t)$，边不相交的 $s-t$ 道路的最多数目为 $p_e(s,t)$。

首先证明 $F=p_e(s,t)$。如果 G 中从 s 到 t 有 $p_e(s,t)$ 条边不相交的道路，则 N 中亦一定有 $p_e(s,t)$ 条边不相交的有向 $s-t$ 道路，每条这样的路可通过单位流。因此 $F\geqslant p_e(s,t)$。反之，设 F 是 N 中 s 到 t 的最大流，其相应的最大流分布将满足任一条边 e，都有 $f(e)=0$ 或 1。当然如果 $f(u,v)=1$ 并且 $f(v,u)=1$，可以认为过 (u,v) 的流为 0，这时并不影响 F 的值。这样 F 可以看成是 N 中 F 个从 s 到 t 的单位流叠加所成，它们分别对应于 G 中的边不相交的道路，于是又有 $F\leqslant p_e(s,t)$，因此 $F=p_e(s,t)$。

由最大流最小割切定理，$F=C(S,\overline{S})$，其中 $s\in S$，$t\in\overline{S}$。在 N 中每条 $s-t$ 道路至少使用了 $(S,\overline{S})$ 里的一条边，而这条 $s-t$ 道路对应了 G 里的一条路 P，P 也至少经过了某条边 (u,v)，在 N 中 (u,v) 是属于割切 $(S,\overline{S})$ 的，移去这些边 G 将成为非连通，因此我们有一个容量为 F 的割切，所以 $c_e(s,t)\leqslant F=p_e(s,t)$。反之，由于每条 $s-t$ 道路至少用到了 G 的边断集里的一条边，且没有两条路经过同一条边，所以 $p_e(s,t)=c_e(s,t)$。定理得证。

定理 6.4.2 G 是 $k-$边连通的，当且仅当任意两点之间至少有 k 条边不相交的道路。

由定理 6.4.1 以及 $k-$边连通的定义即得。

按照定理证明的思路可以设计求图 G 边连通度的算法。

计算 G 的边连通度的算法描述如下：

1. 输入 G 并构造对应的网络 N。
2. 确定 N 中的一个结点 u。
3. $\lambda(G)\leftarrow m$。
4. 对全部 $v\in V-u$ 做
   begin
5. 令 $s=u$，$t=v$，在 N 中，求 s 到 t 的最大流 F。
6. 若 $F<\lambda(G)$，则 $\lambda(G)\leftarrow F$。
   end。
7. 输出 $\lambda(G)$。

网络 N 里各边的容量都是 1，因此在第 5 行计算最大流的结果 F 恰是分离 s 和 t 的最少边数。由于 s 和 t 是任意的，所以容易产生错觉，以为一定要调用 $\frac{1}{2}n(n-1)$ 次最大流算法。但是实际上只需要 $n-1$ 次就够了，这是因为如果 $(S,\overline{S})$ 是某个网络的最小边断集，那么任意的 $v_i\in S$，$v_j\in\overline{S}$，都有 $\lambda(G)=c_e(v_i,v_j)$。它说明，只要选取其中一个特殊结点，比如 u 作为源，其余结点分别作为汇求其最大流就可以了。因此最多有 $n-1$ 个汇，所以第 4 行的描述是正确的。

如果采用 Edmonds－Karp 算法计算最大流，其计算复杂性是 $O(nm^2)$，那么求 G 的边连通度算法的计算复杂度便是 $O(n^2m^2)$。

下面我们再讨论点连通度的判定。

给定一个无向图 G，构造对应的网络 N 如下，对每个点 $v\in V$，对应 N 的两个结点

v'，v''及一条内部边(v',v'')，此外每条边$(u,v)\in G$对应两条外部边(u'',v')和(v'',u')。内部边的容量为1，外部边容量为∞，源是s''，汇为t'。例如图6.9(a)所对应的网络是(b)。设s''到t'的最大流是F，令$P_v(s,t)$是G中点不相交$s-t$道路的最多数目，我们将证明$F=P_v(s,t)$。如果G中有$P_v(s,t)$条不相交的$s-t$道路，相应地在N中也有$P_v(s,t)$条不相交的$s''-t'$道路。因为对于G中的一条路$(s,v_1,v_2,\cdots,t)$，N中就有一条路$(s'',v'_1,v''_1,v'_2,v''_2,\cdots,t')$，而且沿这条路只能运送单位流。因此$P_v(s,t)\leqslant F$。反之，对$N$中的每个容许流分布$f$，由于每个结点的流的上界是1，所以都只会造成每条边e，有$f(e)=0$或1，这样从s''到t'的任何容许流分布都能分解为沿着点不相交的路径运送一个单位流，它们正好对应G中不相交的$s-t$道路，因此$F\leqslant P_v(s,t)$。综上$F=P_v(s,t)$。

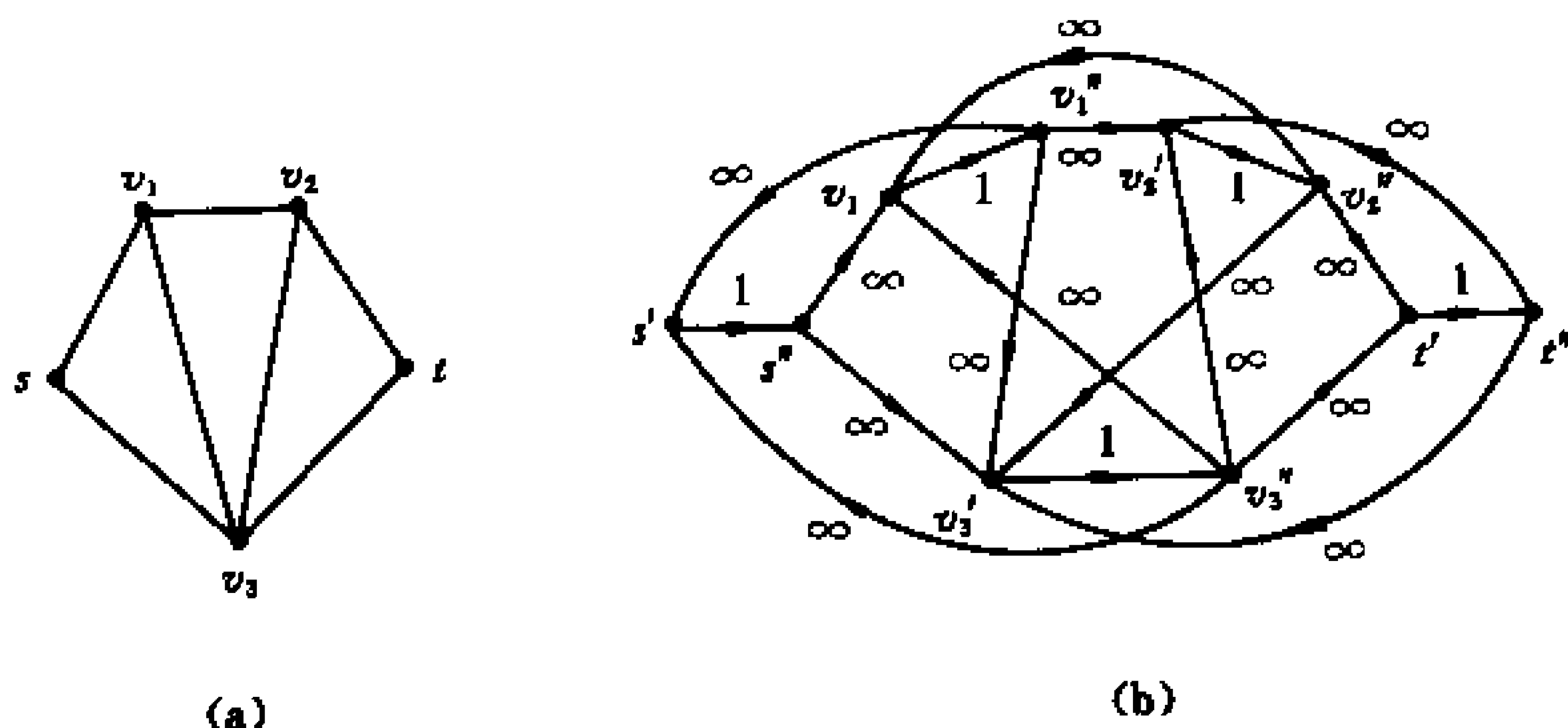


图 6.9

由定理6.3.1和6.3.2可知，G的连通度就是对应网络N中各结点间最大流中的最小值。

G的连通度算法可以描述如下：

1. 输入G并构造相应的网络N。

2. $\kappa(G)\leftarrow n$。

3. $i\leftarrow 0$。

4. While $i\leqslant\kappa(G)$ do

   begin

5. $i\leftarrow i+1$。

6. $for\ j=i+1\ to\ n\ do$

      begin

7. 　　若$(v_i,v_j)\notin E$，求$s=v_i$，$t=v_j$时N的最大流F。

8. 　　若$<\kappa(G)$则$\kappa(G)\leftarrow F$。

      end

   end。

9. 输出$\kappa(G)$。

算法的第1行是从G构造N，如果G有n个结点m条边，则N中就有$2n$个结点，$n+2m$条边，所以构造N的时间复杂性是$O(m)$。

如果令i从1到$n-1$，j从$i+1$到n，在N中分别求从源v_i到汇v_j，满足$(v_i,v_j)\notin$

E 的最大流，据前所述，其中最小值就是 G 的断量。但是算法的第 4 行并没有这样实现，而是当循环体中一旦出现 $i>\kappa(G)$时，即停止执行。其理由如下：

假定一个断集 A 的移去使 $V-A$ 划分为两个结点集 V'，V''，使任何两结点 $v_i\in V'$，$v_j\in V''$，有 $\kappa(G)=P_v(v_i,v_j)$，那么在相应的网络 N 中，V'中的点 v_i''为源，V''中的点 v_j'为汇时一定可求 $\kappa(G)$。这样首先令 v_1 为源 s，分别令 v_2，$v_3\cdots$，v_n 为汇，满足$(v_1,v_j)\notin E$，$j=2$，3，…，n，求 s 到 t 的最大流；然后 v_2 为源，$v_j(j=3,4,\cdots,n)$为汇，当$(v_2,v_j)\notin E$ 时分别求最大流。直至 V_k 为源，此时有 $k=\kappa(G)+1$。由于 $k>\kappa(G)$，显然 v_1，v_2，…，v_k 之中必有一个(比如 v_i)不属于断集，而在这之前已经令 v_i 为源计算过最大流，因此 $\kappa(G)$已经求出，而不必继续判断了。这样改进之后，计算最大流次数的上界是 $\kappa(G)\cdot n$。由定理 6.2.2 可知，其计算复杂性是 $O(m)$。因此如果在第 7 行中采用 Edmonds－Karp 最大流算法，那么该算法的计算复杂性是 $O(nm^3)$。

6.5 无向图的 DFS 算法与图的块划分

在 2.2 节我们曾经简单介绍了 DFS 算法，在以后的一些算法里也采用过它，本节将对它进行更详尽的讨论。

不失一般性，我们假定无向图 G 是连通的。如果不连通，则可以对每个连通分量分别执行 DFS 算法，此外，假定 G 中没有自环。这样，无向图 G 的 DFS 过程是

首先在 G 中任选一点 v，从 v 开始检查，称它是 DFS 的根，然后选择一条边(v,w)，从而访问 v 的一个邻点 w。这时边(v,w)定向为从 v 到 w，称它已检查而且是树边，结点 v 称为 w 的父亲，记为 father(w)。

通常，在检查某结点 x 时，会出现以下两种可能：

1. 与 x 相关联的边都已检查，则回到父亲结点，从 father(x)继续检索。这时称 x 已经完全扫描。

2. 还有与 x 关联的边尚未检查，则选取其中一条边(x,y)，并定向为从 x 到 y，边(x,y)已检查，这时需要考虑两种情况：

a. y 尚未访问过，则访问 y，并从 y 向下检索。此时(x,y)是树边且 $x=$father(y)。

b. y 在前面已经访问过，再选择另一条与 x 相关联同时没检查的边，此时(x,y)称为回退边。

在 DFS 过程中，当结点 x 第一次被访问时，给其赋值 DFN(x)，称为深度优先数。如果 x 是其中第 i 个赋值的结点，则 DFN$(x)=i$。很清楚，它表示了结点在 DFS 中访问的先后顺序。

只有当检索过程又返回到根，而且所有结点都已经访问时，DFS 过程结束。

如前所述，如果 G 是连通图，那么 DFS 过程结束时所有的树边将构成 G 的一棵支撑树，称为 DFS 树，而所有的回退边构成它的余树。例如对图 6.10(a)采用 DFS 算法的结果如(b)所示，其中实线表示树边，而虚线表示余树边。

DFS 算法的形式化描述是：

1. 令 TREE$=\Phi$，BACK$=\Phi$，$i=1$，对 G 的每个结点 v，令 FATHER$(v)=0$，MARK

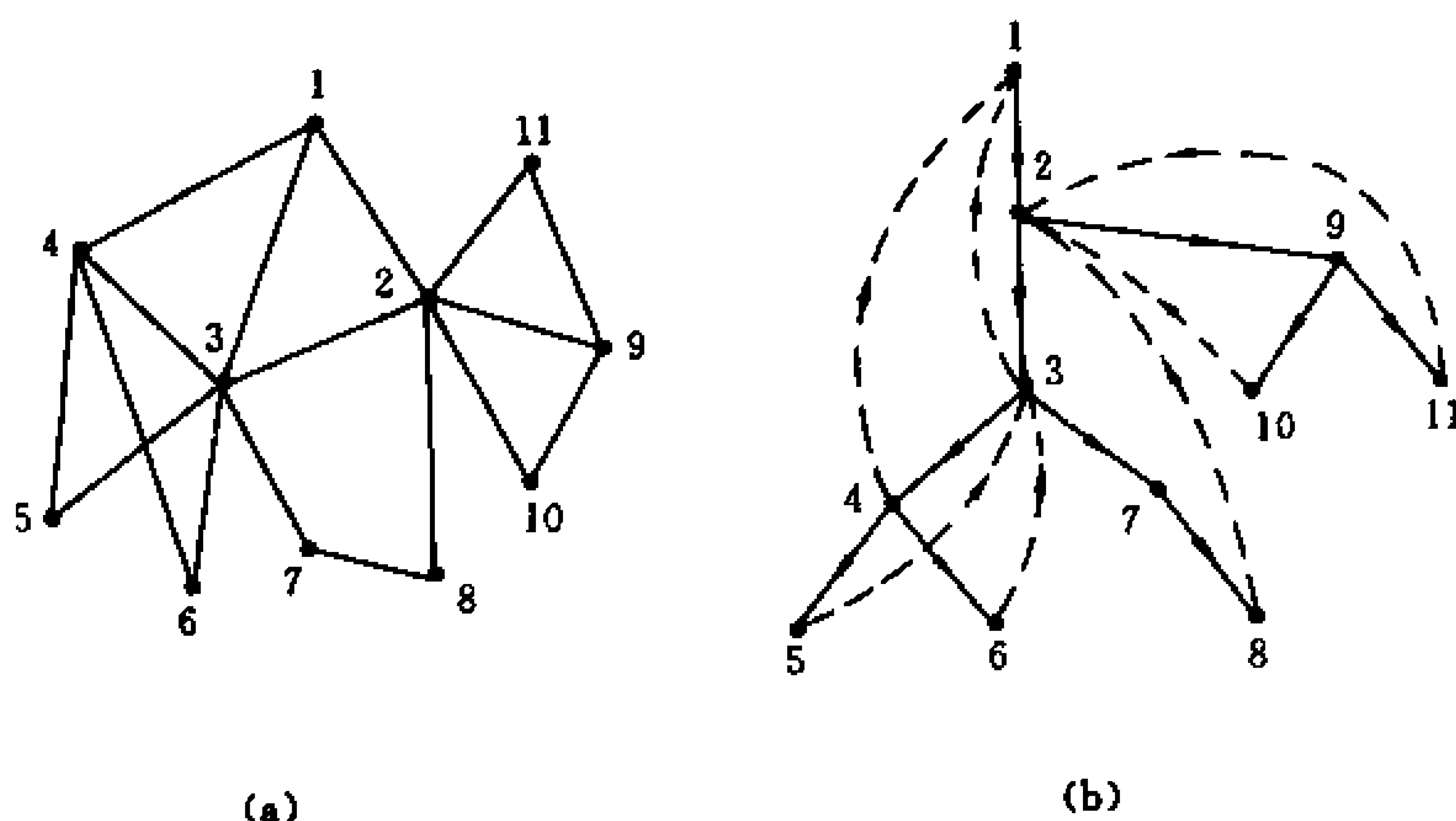


图 6.10

$(v)=0$。

2. 任选一个满足 MARK$(r)=0$ 的结点 r，置 DFN$(r)=i$，MARK$(r)=1$，$v=r$。

3. 如果与 v 关联的边都"已检查"，转 5。否则选一条未查边 (v,w)。

4. 对边 (v,w) 定向为从 v 到 w，并称之"已检查"。

   4.1 若 MARK$(w)=0$，则 $i=i+1$，DFN$(w)=i$，TREE＝TREE $\cup\{(v,w)\}$，MARK$(w)=1$，FATHER$(w)=v$，$v=w$。

   4.2 若 MARK$(w)=1$ 则 BACK＝BACK $\cup\{(v,w)\}$。

   4.3 转 3。

5. 若 FATHER$(v)\neq 0$（即 v 不是根），则 $v=$ FATHER(v)，转 3，否则转 6。

6. 若对所有结点 x，都有 MARK$(x)=1$，转 7，否则 $i=i+1$，转 2（此时 G 不是连通图）。

7. 结束。

算法中，数组 MARK 用来标识各结点是否已访问，TREE 和 BACK 分别用来存放树边和余树边。为了对算法进一步进行分析，我们需要引进若干术语。

如果在 DFS 树 T 中结点 v 到 w 存在一条有向道路，则称 v 是 w 的祖先，或 w 是 v 的子孙。若其中 $v\neq w$，则又称为真祖先和真子孙。如果 $(v,w)\in T$，则说 v 是 w 的父亲，w 是 v 的一个儿子。结点 v 和它的全部子孙构成了 T 的一个子树，v 是这棵子树的根。两个结点 v 和 w，如果其中一个是另一个的子孙，则说它们是有关的，否则是无关的，这时如果 v 比 w 先访问，称 v 在 w 之左。图 G 中无关结点之间的边称为横跨边。现在我们证明无向连通图 G 不存在横跨边。

定理 6.5.1 设 (v,w) 是无向连通图 G 的一条边，则 G 的任一个 DFS 树中，v 和 w 之间必有一个是另一个的子孙。

证明：假定 v 和 w 在 T 中是无关的，则一定存在两个结点 s_1 和 s_2，满足 FATHER$(s_1)=$ FATHER(s_2)，同时 v 和 w 分别是 s_1 和 s_2 的子孙。令 T_1 和 T_2 分别是 T 的以 s_1 和

s_2 为根的子树，不失一般性，设 DFN(s_1)<DFN(s_2)，显然在 DFS 算法中 T_2 的各结点应在 s_1 完全检查之后访问，而只有 T_1 中各结点都完全检查之后，s_1 的扫描才告结束。因此不可能存在 v 到 w 的边。

没有横跨边是无向图 DFS 算法的重要特征，也是下面将要讨论的块划分算法的基础。

根据定义 6.1.2，如果无向连通图 G 不存在割点，那么它就是 2—连通的，若存在割点 v，则 $G-v$ 将分解成若干个连通子图，或者说 G 存在若干块，其中每块都是 G 的最大 2—连通分量。因此一旦确定了割点，也就实现了 G 的块划分。

图的很多算法都与块划分有直接联系，例如判断 G 的最长初级回路，如果预先进行了分块处理，就可能把问题的规模变小从而改善计算复杂性，此外它十分有利于并行处理。因此图的块划分是图算法的一个重要内容。

引理 6.5.1 设 r 是 G 的 DFS 树 T 的根，$v \neq r$ 是割点当且仅当对 v 的某个儿子 s，在 T 中 s 的任何子孙与 v 的真祖先之间没有回退边。

证明：必要性。设 t_1 是 v 的任一真祖先，t_2 是 s 的任一个子孙，则在树 T 中存在从 t_1 到 t_2 的道路，如果 $(t_2,t_1) \in G$，则产生一个包含 v 的回路，这样 $G-v$ 中 t_1 与 t_2 之间仍有道路，因此 v 不是割点。充分性，如果 $(t_2,t_1) \notin G$，则在 G 中 t_1 和 t_2 之间任何道路都经过 v，由于 t_1、t_2 的任意性，所以 v 是割点。

引理 6.5.2 根 r 是 G 的割点当且仅当它有一个以上的儿子。

其证明类似于引理 6.5.1

这样我们对 G 的每个结点 v，赋以值 LOW(v)。

LOW(v)=min({DFN(v)}∪{DFN(w)|存在回退边(x,w)，满足在 T 中 x 是 v 的子孙，w 是 v 的真祖先})。　　(1)

就可以得到

定理 6.5.2 结点 $v(\neq r)$是 G 的割点当且仅当 v 有一个儿子 s，满足 LOW(s)≥DFN(v)。

由于 LOW(v)的值是 v 沿着 DFS 树 T 到它的子孙，并最多包含一条回退边所能到达结点的最小深度优先数，所以式(1)可以改写为

LOW(v)=min({DFN(v)}∪{LOW(s)|s 是 v 的儿子}∪{DFN(w)|(v,w)是回退边}。

它的具体计算步骤如下：

1. 当 v 是第一次被访问时，LOW(v)=DFN(v)。

2. 当回退边(v,w)被检查时，置

$$\text{LOW}(v) = \min(\text{LOW}(v), \text{DFN}(w))。$$

3. 当 DFS 过程对 v 的一个儿子 s 完全扫描后返回到 v 时，置

$$\text{LOW}(v) = \min(\text{LOW}(v), \text{LOW}(s))。$$

至此我们可以形式地描述图的块划分算法

S1. 对 G 的每个结点 v，置 FATHER(v)=0，MARK(v)=0；令 $i=1$，STACK=Φ。

S2. 任意选择一个满足 MARK(r)=0 的结点 r，置

$$\text{DFN}(r) = i, \text{LOW}(r) = i, \text{MARK}(r) = 1, v = r。$$

S3. 如果所有与 v 关联的边都"已检查"，转 S5，否则选一未查边(v,w)，标之"已检查"，并入 STACK，转 S4。

S4. 执行下述内容后返回 S3。

4.1 若 $\mathrm{MARK}(w)=0$，置

$$i = i + 1, \mathrm{DFN}(w) = i, \mathrm{LOW}(w) = i, \mathrm{FATHER}(w) = v,$$
$$\mathrm{MARK}(w) = 1, v = w。$$

4.2 若 $\mathrm{MARK}(w)=1$，置

$$\mathrm{LOW}(v) = \min(\mathrm{LOW}(v), \mathrm{DFN}(w))。$$

S5. 若 $\mathrm{FATHER}(v)\neq 0$，转 S6，否则转 S8。

S6. 若 $\mathrm{LOW}(v)\geqslant \mathrm{DFN}(\mathrm{FATHER}(v))$，则把 STACK 中从栈顶一直到$(\mathrm{FATHER}(v),v)$的全部边移出。(找到了一个块)。

S7. 置

$$\mathrm{LOW}(\mathrm{FATHER}(v) = \min(\mathrm{LOW}(v), \mathrm{LOW}(\mathrm{FATHER}(v)))$$
$$v = \mathrm{FATHER}(v) \quad 转\ S3$$

S8. 结束。

在该算法中，数组 STACK 用来标识 2－连通分量的边。最初 STACK$=\Phi$，每当一条边被检查时，它就进入到 STACK 的顶部。一旦算法中发现 $\mathrm{LOW}(s)\geqslant \mathrm{DFN}(\mathrm{FATHER}(s))=\mathrm{DFN}(v)$时，由定理 6.5.2，$v$ 是割点，进而，如果 s 是具有上述性质的第一个结点，易知 v 与 s 的所有子孙构成了一个块，它们的边恰好处于 STACK 的顶部直至(v,s)。

例 6.5.1 图 6.11(a)的块划分结果如(b)，它共有 3 个 2－连通分量，分别是$\{e_2,e_3,e_4,e_5,e_6\}$，$\{e_1\}$和$\{e_7,e_8,e_9,e_{10},e_{11}\}$。

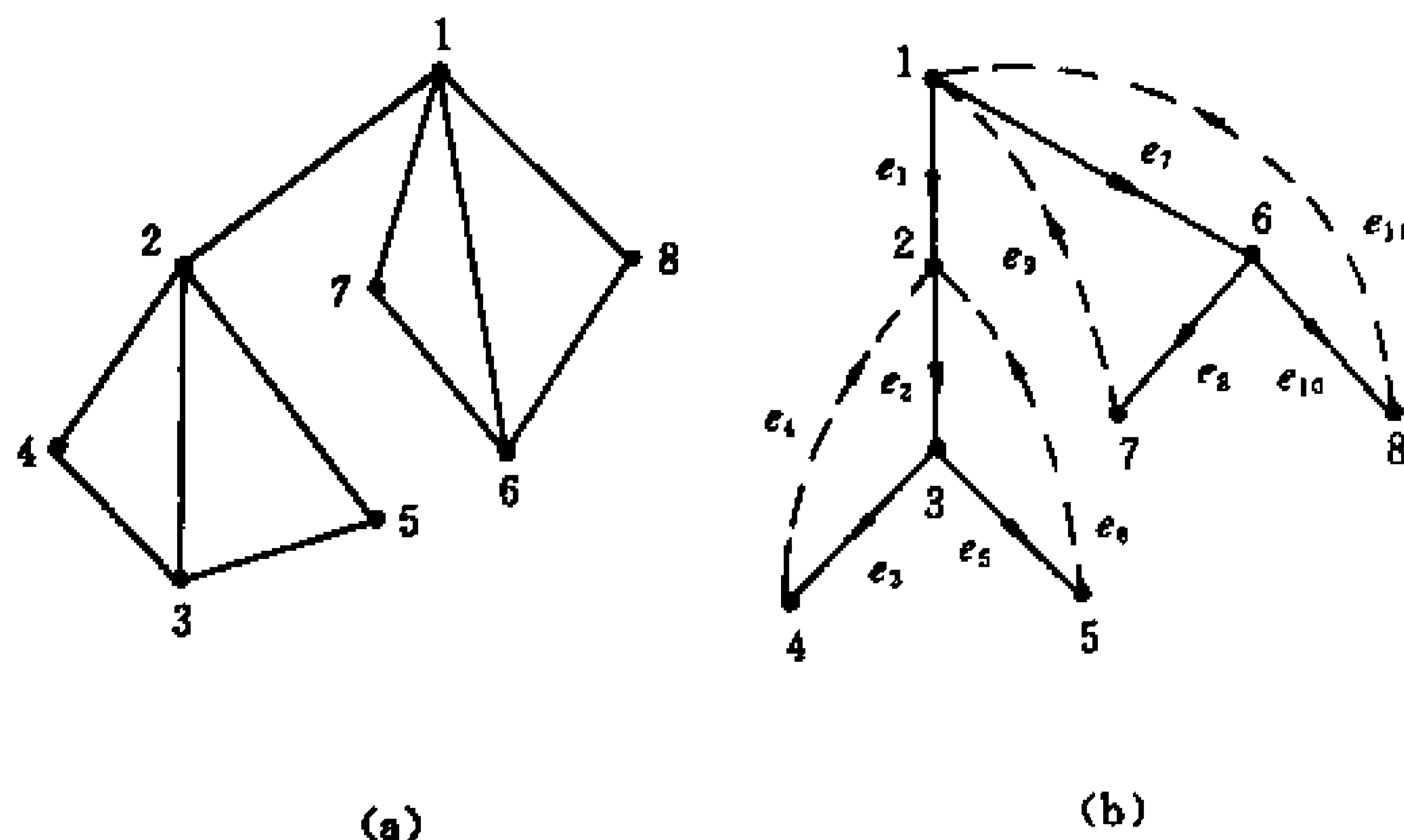


图 6.11

6.6 有向图的 DFS 算法与强连通块划分

有向图的 DFS 算法类似于无向图，但是由于各边方向的限制，所以它会将 G 的诸边划分成四类，当从结点 v 选择一条未检查边(v,w)时，可能

1. w 还没有访问，此时(v,w)是树边。

2. w 已经访问，这时

a. 若 w 是 DFS 森林中 v 的子孙，则(v,w)是向前边。

b. 若 w 是 DFS 森林中 v 的祖先，则(v,w)是回退边。

c. 若 v 和 w 在 DFS 森林中是无关的，且 DFN(w)<DFN(v)，则(v,w)是横跨边。注意，G 中不存在 DFN(w)>DFN(v)的横跨边(v,w)。通过分析不难得到下述几个结论：

1. 如果边(v,w)满足 DFN(w)>DFN(v)，则它不是树边就是向前边。由于通过树边总会访问一个新结点，所以二者容易区分。

2. 若边(v,w)满足 DFN(w)<DFN(v)，则它不是回退边就是横跨边。在检查与 v 关联的边时，如果发现邻点 w 还没有完全扫描，那么(v,w)一定是回退边。

3. 即使 G 是连通的，但其 DFS 森林也可能是非连通的。在 DFS 林每个子树中第一个访问的结点称为该连通分量的根。

在描述有向图 DFS 算法时，我们采用了数组 SCAN，初始对任一结点 v，都有 SCAN $(v)=0$，一旦结点 v 完全扫描，就置 SCAN $(v)=1$。此外还使用两个数组 FORWARD 和 CROSS，它们分别存放向前边和横跨边。

有向图的 DFS 算法如下：

1. 令 TREE=Φ，FORWARD=Φ，BACK=Φ，CROSS=Φ，$i=1$，对 G 中的每点 v，置 MARK $(v)=0$，FATHER $(v)=0$，SCAN $(v)=0$。
2. （确定新根）任选一点 r，满足 MARK $(r)=0$，置 DFN $(r)=i$，MARK $(r)=1$，$v=r$。
3. 若所有以 v 为始点的边都“已检查”，置 SCAN $(v)=1$，转 5。否则选择一条未查边 (v, w) 并转 4。
4. 标边 (v, w)“已检查”，执行以下内容后返回 3。

   4.1 若 MARK $(w)=0$，则

   $i=i+1$，DFN $(w)=i$，TREE=TREE$\cup\{(v, w)\}$，MARK $(w)=1$，FATHER $(w)=v$，$v=w$。

   4.2 否则

   若 DFN (w) >DFN (v)，则 FORWARD=FORWARD$\cup\{(v, w)\}$

   若 DFN (w) <DFN (v) 且 SCAN $(w)=0$，则

   BACK=BACK$\cup\{(v, w)\}$；否则 CROSS=CROSS$\cup\{(v, w)\}$。
5. 若 FATHER $(v)\neq 0$ （v 不是根），则令 $v=$FATHER (v) 并转 3，否则转 6。
6. 若每个结点 x 都有 MARK $(x)=1$，则转 7，否则 $i=i+1$，转 2。
7. 结束。

例 6.6.1 图 6.12 (a) 的 DFS 森林如 (b) 所示，其中实线边是树边，它含有 3 棵子树。

从图中也可以看出，即使 G 是连通的，其 DFS 森林也可能非连通。下面我们将证明，只有强连通图，亦即任意结点到其它各点都存在有向道路时，它的 DFS 森林才是连通的。

定理 6.6.1 强连通图的 DFS 林是连通的。

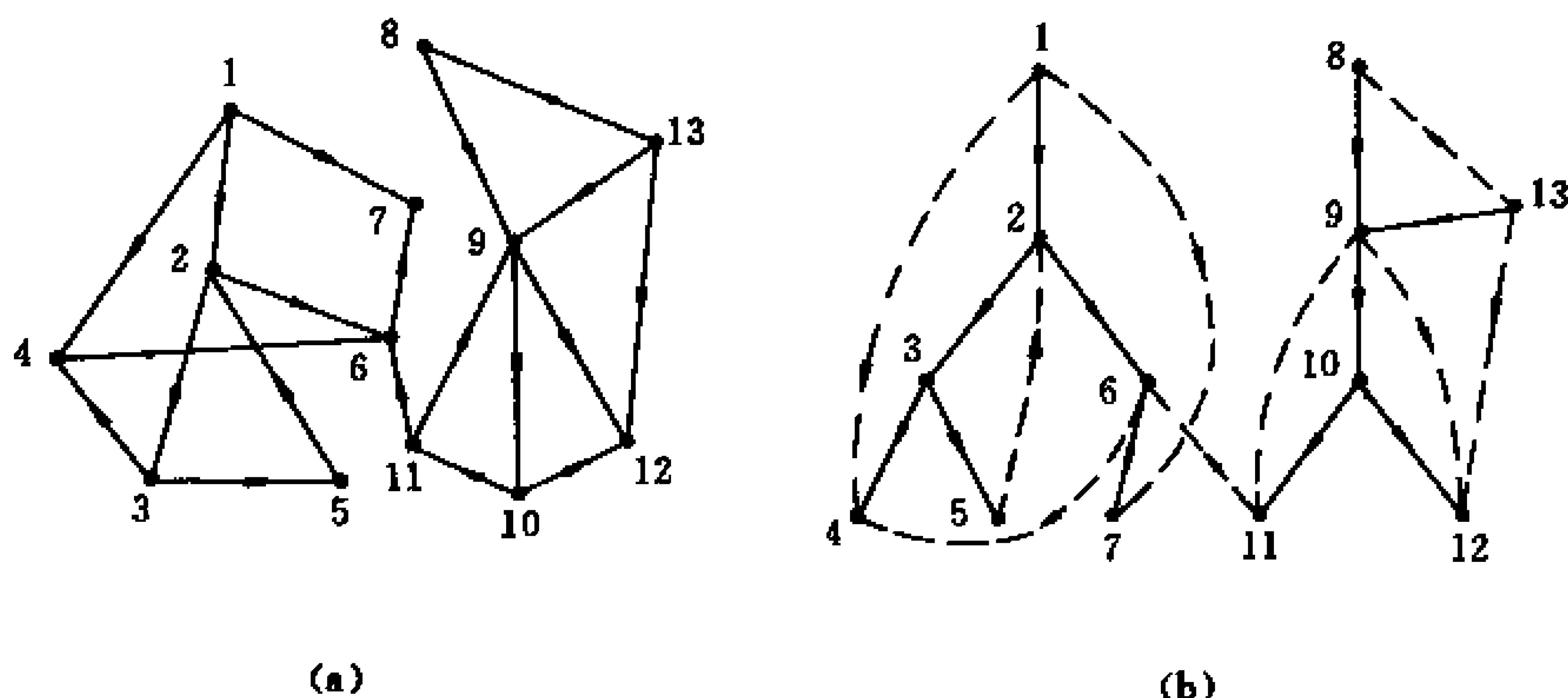


图 6.12

证明：假定 DFS 林不连通，则至少有 2 棵子树 T_1，T_2。设 r_1，r_2 分别是它们的根且 T_1 先得到。由 DFS 过程可知 G 中不存在边 (v, w)，$v \in T_1$，$w \in T_2$，否则必有 $w \in T_1$，这说明在 G 中至少从 r_1 到 T_2 的各结点不存在有向道路，即 G 不是强连通图。

定义 6.6.1 有向图 G 极大的强连通子图称为它的强连通分量，或强连通块。

由定理 6.6.1 可以得到

推论 6.6.1 对应于 G 的强连通分量的 DFS 子树是连通的。

以下我们讨论强连通块算法。

设 $G_1 = (V_1, E_1)$，$G_2 = (V_2, E_2)$，…，$G_k = (V_k, E_k)$ 是 G 的强连通块，T 是 G 的 DFS 林，T_1，T_2，…，T_k 是结点集 V_1，V_2，…，V_k 中 T 的导出子图。由定理 6.6.1，T_i 是连通的。令 r_i $(1 \leqslant i \leqslant k)$ 是 T_i 的根，若 $i < j$，则 DFS 在 v_i 先于 v_j 结束扫描，这说明 r_i 或在 r_j 之左，或是 T 中 r_j 的子孙，而且 G_i 只能由 r_j 的子孙构成，而不可能包含 G_1，…，G_{i-1} 的任何结点。

确定强连通块 G_i 的根 r_i 将是算法的关键，为此我们先分析 G 中诸边之间的关系。

1. 没有 (v, w) 类型的回退边，其中 $v \in V_i$，$w \in V_j$，$i \neq j$，也就是说始点属于 V_i 的回退边，其终点也在 V_i。

2. 没有 (v, w) 类型的横跨边，其中 $v \in V_i$，$w \in V_j$，$i \neq j$，且 r_j 是 r_i 的祖先。这样每条横跨边 (v, w) 只属于下述情形之一。

a. $v \in V_i$，$w \in V_j$，$i \neq j$ 且 r_j 在 r_i 之左。

b. $v \in V_i$，$w \in V_i$。

定义 6.6.2 设 v 是 G 的某个强连通分量 G_i 中的结点，则在 V_i 中 v 沿其有向道路同时最多包含一条回退边或一条横跨边所能到达结点中的最小深度优先数定义为 v 的 LOWLINK 值。亦即

LOWLINK (v) =min（{DFN (v)} ∪ {DFN (w) | v 的子孙到 w 有回退边或横跨边，且 v 与 w 属同一强连通块}）。

这样对 T_i 的根 r_i，有

$$\text{LOWLINK}(r_i) = \text{DFN}(r_i)。$$

假定 $v \in V_i$ 且 $v \neq r_i$，由于它们属于同一强连通块，因此一定有回退边或横跨边 $(v,$

w)，$w \in V_i$，并且满足 DFN（w）<DFN（v），所以

$$\text{LOWLINK}(v) < \text{DFN}(v)。$$

当然，此时 v 也一定有道路 P 可达 r_i，这样我们得到

定理 6.6.2 v 是有向图 G 的一个强连通分量的根，当且仅当 LOELINK（v）=DFN（v）。

LOWLINK（v）的值可以计算如下：

1. 当结点 v 首次访问时，LOWLINK（v）=DFN（v）。
2. 如果回退边（v，w）被查，置
$$\text{LOWLINK}(v) = \min(\text{LOWLINK}(v), \text{DFN}(w))。$$
3. 若（v，w）是横跨边且 v，w 在同一强连通分量，置
$$\text{LOWLINK}(v) = \min(\text{LOWLINK}(v), \text{DFN}(w))$$
4. 当 v 的儿子 s 完全扫描之后返回 v 时
$$\text{LOWLINK}(v) = \min(\text{LOWLINK}(v), \text{LOWLINK}(s))。$$

其中 3 尚需判断 v 和 w 在同一分量，为此采用一个数组 STACK1，按 DFS 的访问次序将结点存入该数组。它不但可以确定强连通分量的全部结点，也能对 3 进行判断，此时如果 w 在 STACK1 之中，那么 v 与 w 属同一强连通块。一旦确定了一个强连通块，那么这些结点都从 STACK1 中移出。为此每个结点可以设置一个 POINT 值，若 v 在 STACK1 之中，则 POINT（v）=1，否则 POINT（v）=0。

下面我们给出强连通块划分算法：

S1 对 G 中每个结点 v，置

$$\text{MARK}(v) = 0, \text{FATHER}(v) = 0, \text{POINT}(v) = 0; i = 1,$$
$$\text{STACK1} = \Phi。$$

S2 任选一点 r，满足 MARK（r）=0，置

$$\text{DFN}(r) = i, \text{LOWLINK}(r) = i, \text{MARK}(r) = 1$$
r 进入 STACK1，$\text{POINT}(r) = 1, v = r$。

S3 如果以 v 为始点的所有边都"已检查"，转 S5；否则选一条未查边（v，w），标之"已检查"并转 S4。

S4 执行以下内容后返回 S3。

1. 若 MARK（w）=0，则 $i=i+1$，DFN（w）=i，LOWLINK（w）=i，FATHER（w）=v，MARK（w）=1
   w 进入 STACK1，POINT（w）=1，$v=w$
2. 若 MARK（w）=1，DFN（w）<DFN（v）及 POINT（w）=1，
   则 LOWLINK（v）=min（LOWLINK（v），DFN（w））。

S5 若 LOWLINK（v）=DFN（v），则移去 STACK1 中从栈顶直至 v 的全部结点（它们构成一个强连通块），且对所有这些结点 x，置 POINT（x）=0。

S6 若 FATHER（v）=0。转 S7，否则
LOWLINK（FATHER（v））=min（LOWLINK（FATHER（v）），LOWLINK（v））。

v=FATHER (v)，转 S3

S7 若所有结点 $x \in V$ 都有 MARK (x) =1，转 S8，否则转 S2。

S8 结束。

例 6.6.2 图 6.13 给出了强连通块判断算法的说明。其中 LOWLINK 值在括号中给出。该图共有 4 个强连通分量，它们分别是 {3, 4, 5}, {6, 7, 8, 9, 10}, {2} 和 {1, 11, 12, 13}。

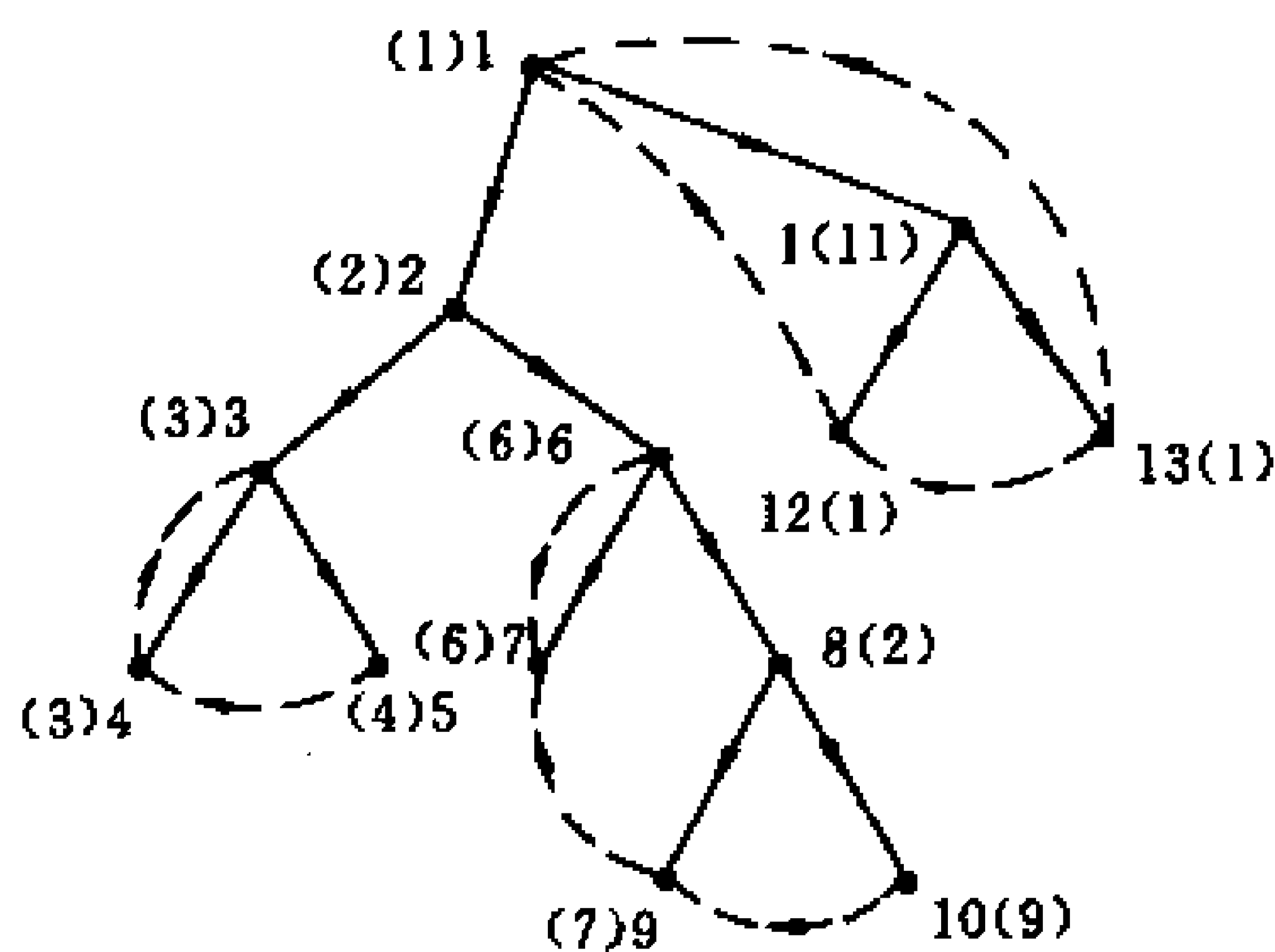
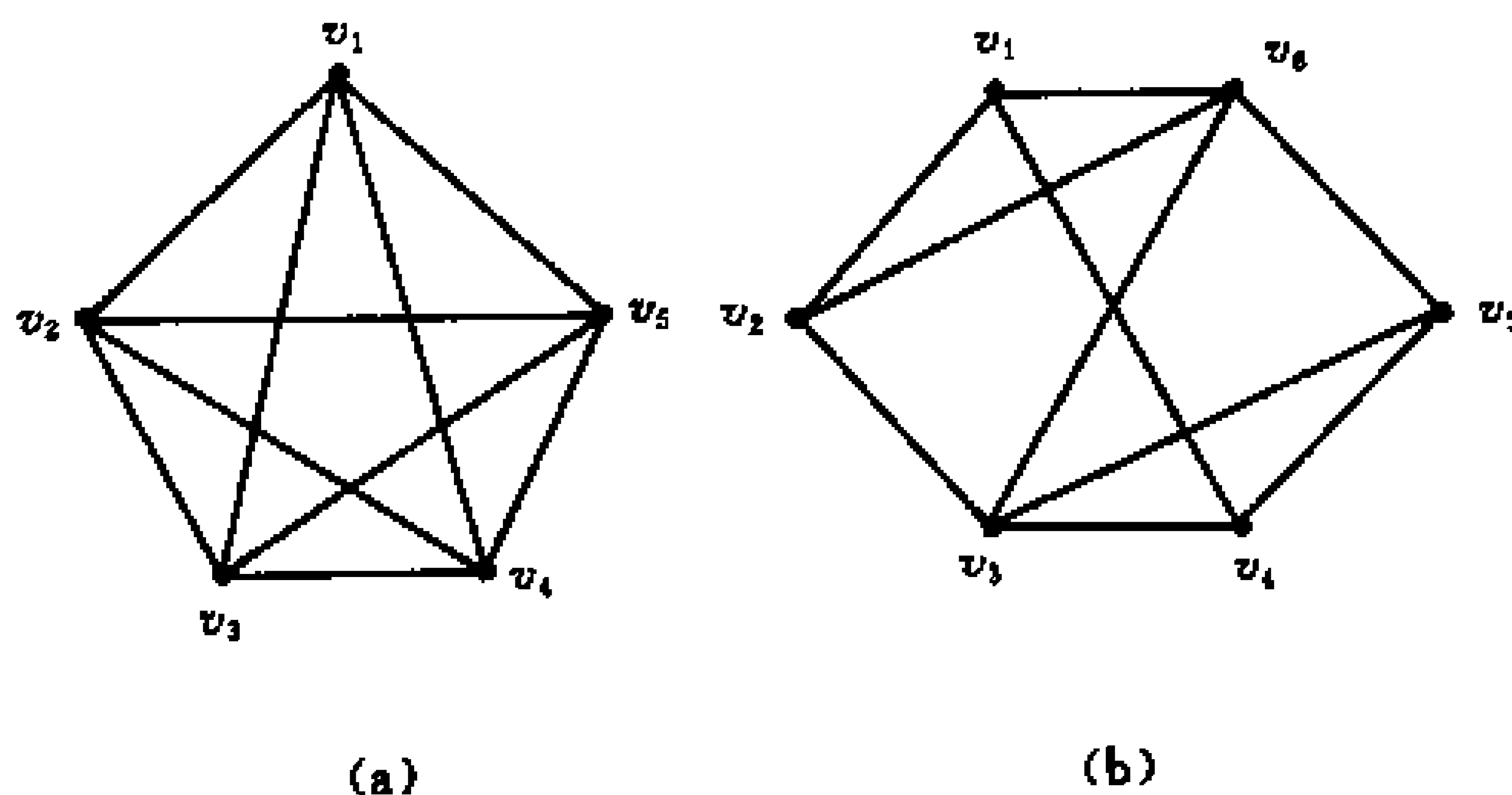


图 6.13

习 题 六

1. 一个有 n 个结点的图最多有多少个割点，多少条割边？
2. 证明若 v 是简单图 G 的割点，则 v 一定不是补图 G 的割点。
3. 试给出下图的二个断集和边断集，并求 κ (G) 和 λ (G)



题图 6.3

4. 证明：当且仅当 G 的任意两结点间至少有两条不相交的道路时，G 才是 2—连通的。

5. 不利用定理 6.2.4，证明：若 G 是 n 个结点的简单图，$d(v_1) \leqslant d(v_2) \leqslant \cdots \leqslant d(v_n)$，且满足

$$d(v_k) \geqslant k, \qquad 1 \leqslant k \leqslant n-1-d(v_n)。$$

则 G 是连通图。

6. 设 G 是不只含一个回路的 2—连通图，证明 G 中一定存在内部结点度都为 2 的道路 P（P 中若有内部结点，则其度都为 2），使 $G-P$ 仍是 2—连通的。

7. 设 G 是 3—连通图，给定连接 u 和 v 的不相交道路 P_1 和 P_2，问是否总可以找到

第三条道路 P_{uv}，它与 P_1，P_2 也不相交？

8. 试证明有向图 DFS 算法的计算复杂性。

9. 证明有向图 G 中不存在 DFN（w）>DFN（v）的横跨边（v，w）。

10. 设 T 是 G 的 DFS 树，G_i 是 G 的完全子图，证明 G_i 的所有结点都处于 T 的同一条有向道路上。

11. 设 T 是有向图 G 的 DFS 林，若 C 是 G 中的一个有向回路且 v 是 C 中深度优先数最小的结点，证明 v 是 T 中 C 上各结点的祖先。

12. 编程实现边连通度算法。

13. 编程实现点连通度算法。

14. 编写连通图 G 块划分的程序。

15. 编写有向连通图 G 强连通块判定的程序。

第七章　代数结构预备知识

7.1 集合与映射

读者已熟知有关集合的一些基本概念及记号，本节只补充关于集合幂集的概念。

设 S 是任意一个集合，如果元素 a 属于 S，记为 $a\in S$，否则记 $a\notin S$。S 中不同元素的个数称为该集合的基数，用 $|S|$ 表示。

当集合 S 确定之后，能相应地得到另一个集合 $\rho(S)$，称为 S 的幂集。$\rho(S)$ 是 S 的全部子集的集合。例如设 $S=\{a,b,c\}$，则

$\rho(S)=\{\phi,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},S\}$。

如果 S 是有限集，容易证明幂集 $\rho(S)$ 的基数是 $2^{|S|}$，也就是说 S 有 $2^{|S|}$ 个不同的子集。对于其中某一个子集 A，可以刻划成

$$A=\{x\in S|P(x)\},$$

即是 S 中有性质 P 的全部元素组成的集合。

例 7.1.1　设 $S=\{1,2,\cdots,18\}$，则 $A=\{x\in S|3|x\}$ 是 S 中全部能被 3 整除的元素构成的集合。因此 A 也可以表示为

$$A=\{3,6,9,12,15,18\}。$$

再如若

$$B=\{x\in S|3|x \text{ 或 } 5|x\},$$

那么 B 是 S 中能被 3 或 5 整除的全部元素构成的集合，亦即

$$B=\{3,5,6,9,10,12,15,18\}。$$

例 7.1.2　设 Z 表示整数集，则

$$N=\{x\in Z|x\geqslant 0\}$$

定义了 Z 的非负整数子集。

设 A 和 B 都是 S 的子集，如果 A 是 B 的子集，即 A 的元素也都是 B 的元素，亦即 $a\in A\Rightarrow a\in B$，记作 $A\subseteq B$。如果 $A\subseteq B$ 且 $B\supseteq A$，则称两个集合是相等的，记作 $A=B$。由全部既属于 A 又属于 B 的元素组成的集合称为 A 和 B 的交集，用 $A\cap B$ 表示。若 A 和 B 没有共同的元素，则 $A\cap B=\varnothing$。A 和 B 的并集是由属于 A 或属于 B 的全部元素组成的集合，记作 $A\cup B$。自然，$A\cap B$ 和 $A\cup B$ 仍然是 S 的子集。

集合的交并运算的一个重要性质是适合分配律，即

$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)。\qquad(1)$$

$$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)。\qquad(2)$$

定义 7.1.1　设 S 和 T 是给定的两个集合，如果有一个规则 f，使对任意一个元素 $X\in S$，在 T 中有唯一的元素 y 与之对应，则称 f 是 S 到 T 的一个映射。记作 $f:S\to T$ 和 $y=f(x)$，S 称为 f 的定义域，T 称为 f 的值域，y 称为 x 的象，x 称为 y 的原象。

直观上可以把映射看成是一种输入输出关系如图 7.1 对每一个输入 $s\in S$，通过映射 f 产生唯一的输出 t。

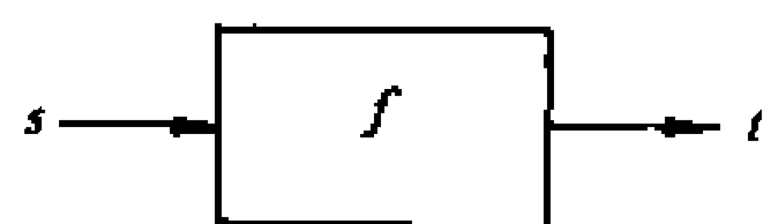


图 7.1

根据定义，S 中任意元素在 T 中都有象，但 T 中的每个元素在 S 中不一定都有原象。习惯上我们将 S 中全部元素的象所构成的集合称为 f 的象，记作 $f(S)$。显然 $f(S)\subseteq T$。

例 7.1.3 设 $S=\{a,b,c\}$，$T=\{1,2,3\}$。

$$f_1: a\to 1,\ b\to 2,\ c\to 3,$$

是 S 到 T 的一个映射。

$$f_2: a\to 1,\ b\to 2,\ c\to 2,$$

是 S 到 T 的一个映射。

例 7.1.4 设 A 是非负整数集，$B=\{x|x$ 是非负偶数$\}$

$$g:\begin{cases} n\to n, & \text{当 } 2|n \text{ 时}, \\ n\to n+1, & \text{当 } 2|n \text{ 时}, \end{cases}$$

是 A 到 B 的一个映射。

例 7.1.5 设 A 为一个非空集合。

$$I_A: a\to a, \forall a\in A,$$

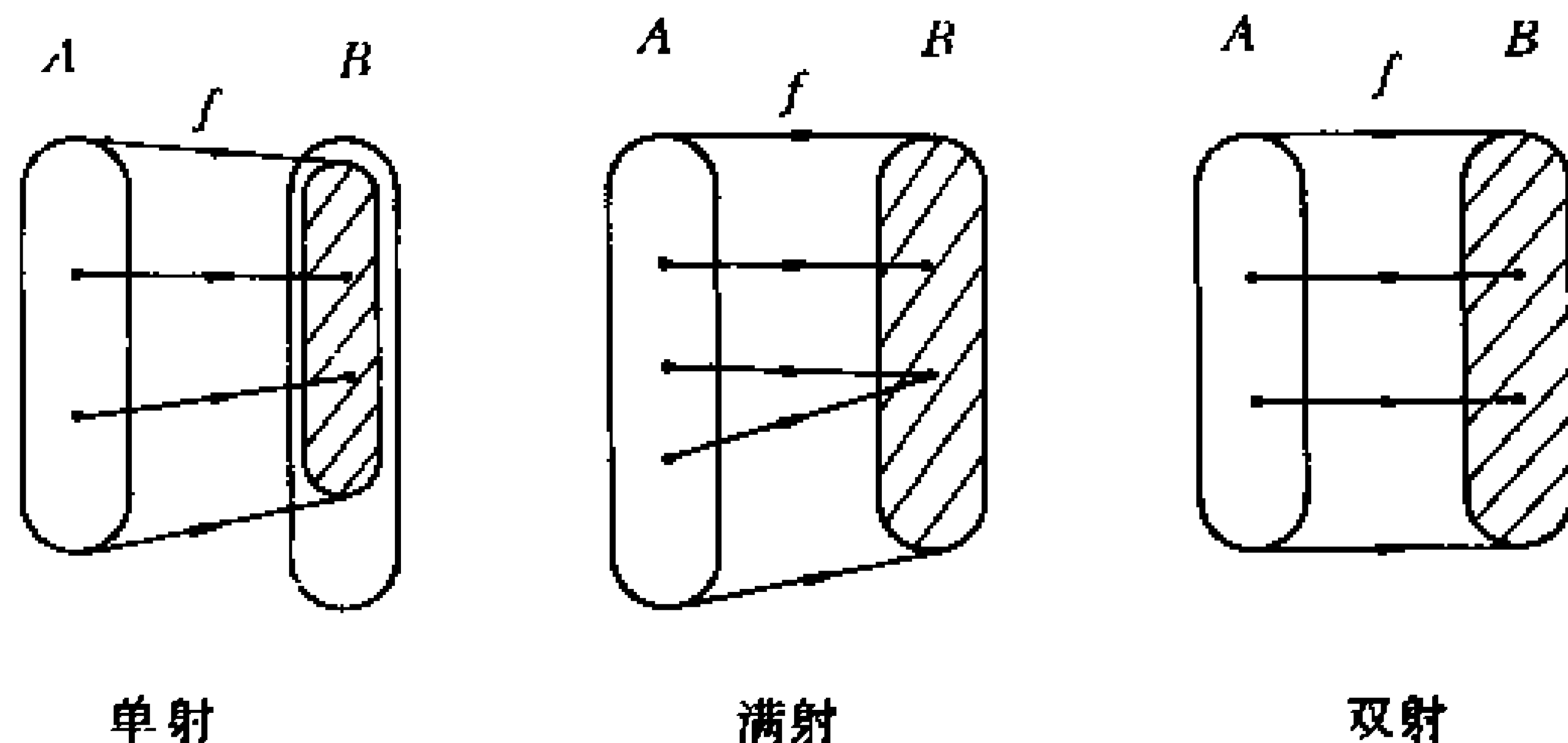
是 A 到 A 的一个映射，称为 A 上的恒等映射或单位映射。

定义 7.1.2 两个映射 f,g，$f:A_1\to B_1$，$g:A_2\to B_2$，当且仅当 $A_1=A_2$，$B_1=B_2$，且对任意 $x\in A$，都有 $f(x)=g(x)$，称 f 和 g 是相等的映射，记为 $f=g$。

定义 7.1.3 设 f 是 A 到 B 的一个映射。

1. 若对任意 $a_i\neq a_j$，$a_i,a_j\in A$，都有 $f(a_i)\neq f(a_j)$，称 f 是 A 到 B 的单射。
2. 若 $f(A)=B$，则称 f 是 A 到 B 的满射。
3. 若 f 既是单射又是满射，则称它是 A 到 B 的双射。

例 7.1.3 的 f_2 不是单射也不是满射，f_1 是双射。例 7.1.4 的 g 是满射，但不是单射。例 7.1.5 的 I_A 是双射。也就是说，若 f 是 A 到 B 的单射，它一定把 A 中的不同元素映射到 B 中的不同元，即若 $a_1\neq a_2$，则 $f(a_1)\neq f(a_2)$；若 f 是满射，那么对于 B 中的每一个元素 b，在 A 中至少有一个 b 的原象；如果 f 是双射，那么 A 与 B 的元素之间由 f 构成了一一对应，因此双射亦称为一一对应映射。它们的直观意义如图 7.2 所示：



单射　　满射　　双射

图 7.2

在映射之间能够定义合成运算。

定义 7.1.4 设 A、B、C 是三个集合，有两个映射：$f:A\to B$，$g:B\to C$，则由 f 和 g 可确定一个 A 到 C 的映射 h，$h:a\to g(f(a))$，称 h 为 f 与 g 的合成，记作 $h=gf$，亦即

$$h(a)=(gf)(a)=g(f(a))。$$

h 可用图 7.3 表示。

映射的合成一般不满足交换律，但满足结合律。例如设 $A\to B$，$B\to C$，$C\to D$，两个合成映射 $\gamma(\beta\alpha)$ 与 $(\gamma\beta)\alpha$ 有同样的定义域 A 和值域 D，而且对任意 $a\in A$，有

$$(\gamma(\beta\alpha))(a)=\gamma((\beta\alpha)(a))=\gamma(\beta(\alpha(a)))。$$

$$((\gamma\beta)\alpha)(a)=(\gamma\beta)(\alpha(a))=\gamma(\beta(\alpha(a)))。$$

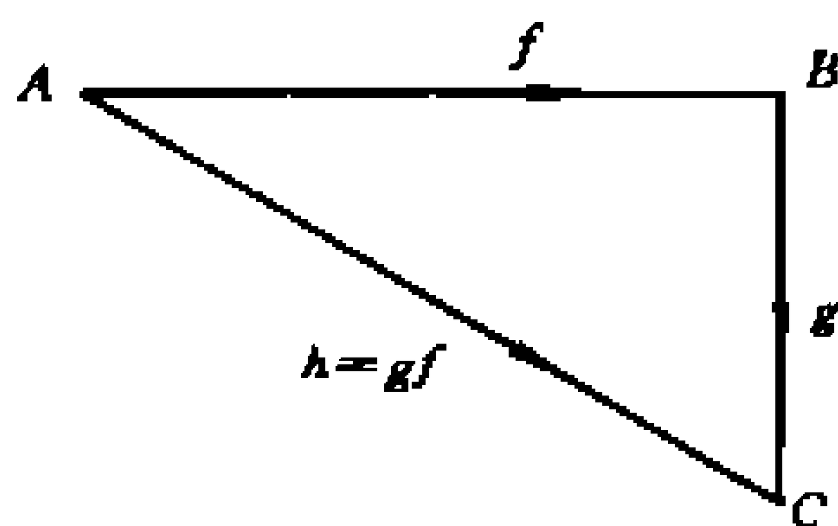


图 7.3

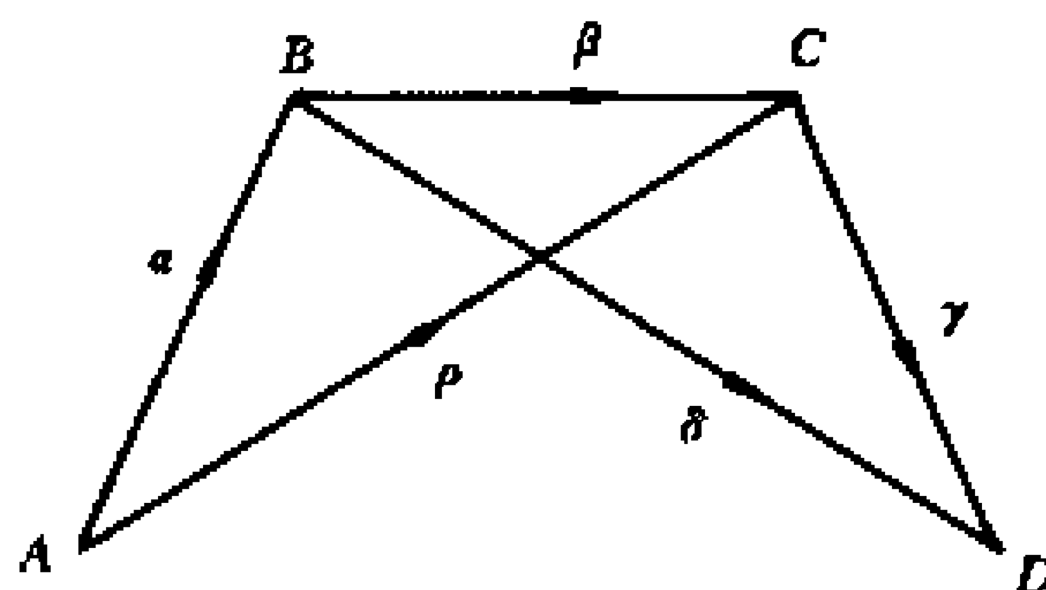


图 7.4

因此 $\gamma(\beta\alpha)=(\gamma\beta)\alpha$。这也可以用图 7.4 说明。图中三角形 ABC 和 BCD 是传递的，因此

$$\gamma(\beta\alpha)=\gamma\rho=\delta\alpha=(\gamma\beta)\alpha。$$

映射图对我们分析映射是有帮助的。

定理 7.1.1 设 f 是 A 到 B 的映射，I_A 和 I_B 分别是 A 与 B 中的恒等映射，则

$$I_Bf=f,\quad fI_A=f。$$

证明：I_Bf 和 f 的定义域都是 A，值域是 B，并且对任意 $a\in A$，都有

$$I_Bf(a)=I_B(f(a))=f(a),$$

故 $I_Bf=f$。同理可证 $fI_A=f$。

定义 7.1.5 设两个映射 $f:A\to B$，$g:B\to A$，若 $gf=I_A$ 成立，则称 f 是左可逆映射，g 是右可逆映射，并称 g 是 f 的左逆映射，f 是 g 的右逆映射。又若 $fg=I_B$ 也成立，则称 f 和 g 都是可逆映射。

定理 7.1.2 A 到 B 的映射 f 是左可逆的充要条件是 f 为单射，f 是右可逆的充要条件是 f 为满射。

证明：因为 f 左可逆，所以存在 $g:B\to A$，使 $gf=I_A$，如果 $f(a_1)=f(a_2)$，一定有 $a_1=a_2$，那么 f 就是单射，由于

$$\begin{aligned}a_1&=I_A(a_1)=gf(a_1)=g(f(a_1))=g(f(a_2))\\&=gf(a_2)=I_A(a_2)=a_2。\end{aligned}$$

所以 f 是单射。

反之设 $A\to B$ 是单射，定义 $g:B\to A$ 如下

$$g(b)=\begin{cases}a,\ 若存在\ a\in A,使\ f(a)=b。\\ a_0,\ 若\ b\notin f(A)\ 且\ a_0\in A。\end{cases}$$

这样对任意 $b\in B$,$g(b)$ 都唯一的确定,所以 g 是一个映射,并且对任意 $a\in A$,有

$$gf(a) = g(f(a)) = g(b) = a。$$

即 $gf = I_A$,因此 f 有左逆映射。定理后半部分的证明留作练习。

推论:$f:A\to B$ 是可逆映射,当且仅当 f 是双射。

定理 7.1.3 设 f 是 A 到 B 的映射,且 $gf = I_A$,$fh = I_B$,则 $g = h$。

证明:

$$g = gI_B = g(fh) = (gf)(h) = I_Ah = h。$$

这说明可逆映射 f 的逆映射是唯一的,通常用 f^{-1}表示,容易证明$(f^{-1})^{-1}=f$ 。

例 7.1.6 设 $f:A\to B$,$g:B\to C$ 都是双射,则 gf 是 A 到 C 的双射。

证明:由定理 7.1.2 的推论,有逆映射 $f^{-1}:B\to A$,$g^{-1}:C\to B$,因此 $f^{-1}g^{-1}$是 C 到 A 的映射,并且

$$(gf)(f^{-1}g^{-1}) = ((gf)f^{-1})g^{-1} = (g(ff^{-1}))g^{-1} = gg^{-1} = I_C。$$

$$(f^{-1}g^{-1})(gf) = f^{-1}(g^{-1}(gf)) = f^{-1}((g^{-1}g)f) = f^{-1}f = I_A。$$

因此 gf 是可逆映射,$f^{-1}g^{-1}$是它的逆。所以 gf 是双射。

由该例和定理 7.1.3 可知 $(gf)^{-1} = f^{-1}g^{-1}$。

7.2 等 价 关 系

集合 A 到 B 的任何映射 f 都是定义域为 A 的 $A\times B$ 的子集。可以将映射的概念加以推广,即其定义域不一定是 A 本身,这就是二元关系。

定义 7.2.1 集合 A 和 B 的笛卡儿积 $A\times B$ 的任一子集 R 称为 A 与 B 之间的一个二元关系,它的元素是有序对 (a,b),记为 $a\,R\,b$,其中 $a\in A$,$b\in B$。当 $(a,b)\notin R$ 时,说 a 与 b 没有 R 关系,记作 $a \not R b$ 。

下面着重讨论集合 A 上的等价关系。

定义 7.2.2 设 R 是集合上的二元关系,如果

1. 对所有的 $a\in A$,都有 $a\,R\,a$,即 R 具有自反性;

2. 对所有的 $a,b\in A$,若 $a\,R\,b$,则 $b\,R\,a$,即 R 具有对称性;

3. 对所有的 $a,b,c\in A$,若 $a\,R\,b$,$b\,R\,c$,则 $a\,R\,c$,即 R 具有传递性。

则称 R 是 A 上的等价关系。用符号 $\sim$ 表示。

集合中的等价关系与该集合的划分有密切联系。设 R 是 A 上的一个等价关系,则 A 中的任意两个元素 a,b 之间或者有 R 关系,或者没有 R 关系,即 $a\,R\,b$,或 $a \not R b$,二者必居其一。这样,对任一元素 $a\in A$,可以把所有与 a 有 R 关系的元素构成一个集合,称之为 A 的一个等价类,记作 $\bar{a}$,即

$$\bar{a} = \{ x\in A \mid x \sim a \},$$

其中 a 是该等价类 $\bar{a}$ 的代表元。

依据等价关系的定义,等价类 $\bar{a}$ 具有以下性质:

1. $a\in\bar{a}$。

2. 若 $b,c\in\bar{a}$,则 $b\sim c$。

3. 若 $b\in\bar{a}$ 且 $b\sim x$，则 $x\in\bar{a}$

定理 7.2.1 设 $\sim$ 是 A 上的一个等价关系，对任意元素 $a,b\in A$，若非 $\bar{a}=\bar{b}$，则有 $\bar{a}\cap\bar{b}=\phi$。

证明从略，由它可以得出如下定理：

定理 7.2.2 设 $\bar{a}_1,\bar{a}_2,\cdots,\bar{a}_n$ 是 A 上由等价关系 $\sim$ 确定的全部等价类，那么

$$\bigcup_{i=1}^{n}\bar{a}=A,\quad \bar{a}_i\bigcap_{i\neq j}\bar{a}_j=\phi。$$

该定理说明等价关系 $\sim$ 确定了集合 A 的一个划分。我们把由 $\sim$ 确定的等价类的集合称为等价类族，用 $\bar{A}$ 表示，即

$$\bar{A}=\{\bar{a}|a\in A\}。$$

为了表示等价类族是由等价关系 $\sim$ 确定的，常常使用记号 $A/\sim$ 表示 $\bar{A}$，并称之为 A 关于 $\sim$ 的商集。

例 7.2.1 设 A 是图 7.5 坐标平面上水平线中所有点的集合，如果 a 和 b 处于同一水平线上，则 $a\,R\,b$，可见 R 是 A 中的一个等价关系。其中每一条水平线都是 R 的一个等价类，A/R 是所有这些水平线的集合。

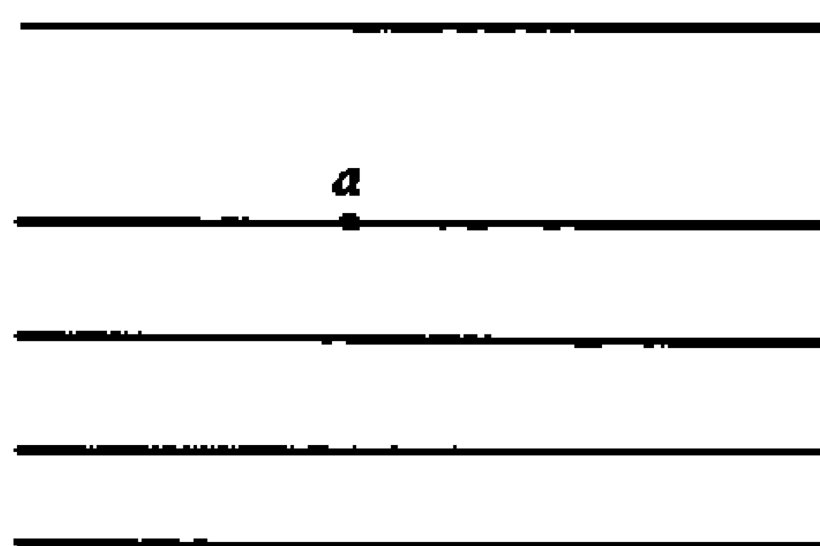


图 7.5

例 7.2.2 设 $A=\{0,1,2,\cdots\}$是非负整数集合，m 是一个正整数，令 R 是 A 中的模 m 同余关系。则

$$\bar{1}=\{1,m+1,2m+1,\cdots\},$$
$$\bar{2}=\{2,m+2,2m+2,\cdots\},$$
$$\cdots\qquad\cdots$$
$$\overline{m-1}=\{m-1,2m-1,3m-1,\cdots\},$$
$$\bar{0}=\{0,m,2m,\cdots\}。$$

显然 R 是等价关系，因此

$$A/R=\{\bar{0},\bar{1},\cdots,\overline{m-1}\}。$$

商集 $A/\sim$ 确定以后，对每一个 $a\in A$，都对应 $A/\sim$ 中的某个确定元 $\bar{a}$，因此 $\gamma:a\to\bar{a}$ 是 A 到 $A/\sim$ 的一个映射，称它是 A 到 $A/\sim$ 的自然映射，很明显 γ 是满射。

集合 A 上的等价关系 $\sim$ 可以确定 A 的一个划分，即 $A/\sim$。反之，如果已经知道 A 的某个划分 B，能不能由它来确定 A 的一个等价关系呢？对此有结论

定理 7.2.3 集合 A 的一个划分可以确定 A 的一个等价关系。

利用映射的概念，我们可以得到如下定理。

定理 7.2.4 设 f 是 A 到 B 的一个满射，则 f 可以确定 A 的一个等价关系。

证明：任取 $b\in B$，因为 f 是满射，所以 b 的原象 $f^{-1}(b)=\{a\in A|f(a)=b\}$是 A 的一个非空子集。因此 $\bigcup_{b\in B}f^{-1}(b)=A$，同时对 $b_1\neq b_2$，有 $f^{-1}(b_1)\cap f^{-1}(b_2)=\Phi$，否则 f 不是映射，因此 $f^{-1}(b_i)\bigcap_{b_i\neq b_j}f^{-1}(b_j)=\Phi$，由上可知 $\{f^{-1}(b)|b\in B\}$ 是 A 的一个划分，由定理 7.2.3，即 f 可以确定 A 上的一个等价关系 $\sim$。

定理 7.2.5 设 f 是 A 到 B 的一个满射，则存在唯一双射 $f^*:A/\sim\to B$，使 $f=f^*\gamma$，其中 $\sim$ 是由 f 确定的等价关系，γ 是 A 到 $A/\sim$ 的自然映射。

该定理的直观意义如图7.6所示。

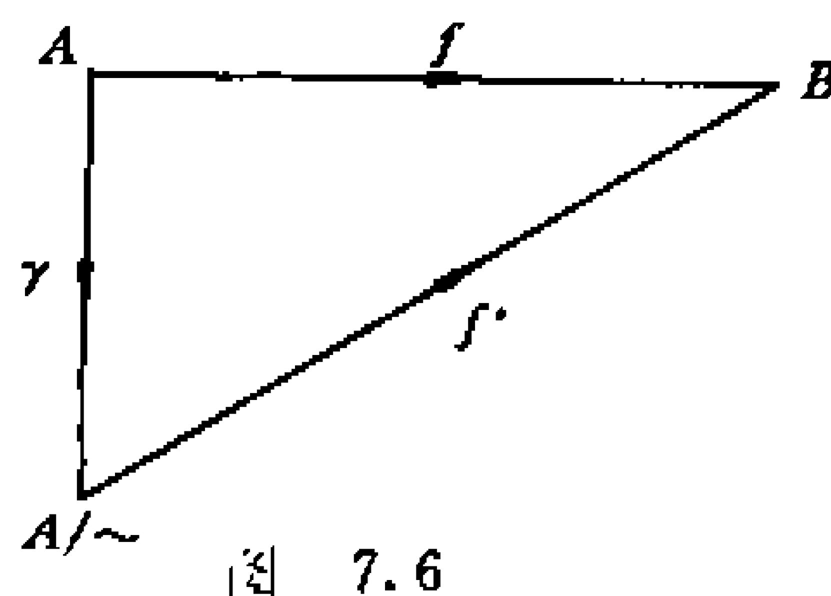


图 7.6

证明：设由 f 确定的等价关系为 $a_1 \sim a_2 <=> f(a_1) = f(a_2)$，而且 $f(a) = b$，可以判定，对任意的 $\bar{a} \in A/\sim$，$f^*:\bar{a} \to b$ 是 $A/\sim$ 到 B 的一个双射。

若 $\bar{a}_1 = \bar{a}$，则 $a_1 \sim a$，即 $f(a_1) = f(a) = b$，所以 $\bar{a}$ 的象与 $\bar{a}$ 中的代表元的选择无关，而且对任意的 $\bar{a} \in A/\sim$，都有 $f^*(\bar{a}) = b$，因此 f^* 是 $A/\sim$ 到 B 的一个映射。其次由于 f 是满射，故对任意 $b \in B$ 都有 $f(a) = b$，从而 $f^*(\bar{a}) = b$，即 f^* 是满射。再次，若 $\bar{a}_1 \neq \bar{a}_2$，则其代表元 $a_1 \neq a_2$，亦即 $f(a_1) \neq f(a_2)$，于是可得 $f^*(\bar{a}_1) \neq f^*(\bar{a}_2)$，因此 f^* 是单射，故 f^* 是 $A/\sim$ 到 B 的双射。

对任意 $a \in A$，若 $f(a) = b$，就有 $f^{-1}(b) = a$，由于 γ 是自然映射，因此 $\gamma(a) = \bar{a}$，所以

$$(f^*\gamma)(a) = f^*(\gamma(a)) = f^*(\bar{a}) = b = f(a)。$$

亦即 $f^*\gamma = f$。

再证 f^* 的唯一性。假定存在另一个 $A/\sim$ 到 B 的映射 g^*，$g^* \neq f^*$ 且满足 $f = g^*\gamma$，那么至少存在一个元素 $a \in A$，使 $g^*(\bar{a}) \neq f^*(\bar{a})$，设 $f(a) = b$，且 $(f^*\gamma)(a) = f^*(\gamma(a)) = f^*(\bar{a}) = b = f(a)$，但 $g^*\gamma(a) = g^*(\gamma(a)) = g^*(\bar{a}) \neq b$，因此与 $f = g^*\gamma$ 矛盾，所以 f^* 是唯一的。

例 7.2.3 设 N 是非负整数集，$B = \{0,1,2,3,4,5\}$，$f:n \to r$，r 是 n 模6后的非负余数。显然 f 是 N 到 B 的一个满射。这时 f 决定的 N 的等价关系 $\sim$ 是模6同余关系。因此

$$N/\sim = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}。$$

这时 N 到 $N/\sim$ 的自然映射是 $\gamma:n \to \bar{n}$。而由 f 导出的双射 f^* 是 $f^*:\bar{n} \to r$。即对任意 $n \in N$ 都有

$$(f^*\gamma)(n) = f^*(\gamma(n)) = f^*(\bar{n}) = r = f(n)。$$

所以 $f = f^*\gamma$。

7.3 代数系统的概念

本节讨论一般的代数系统的基本概念，这些概念在后续章节中讨论特定的代数系统时要反复用到。首先给出代数运算的定义。

定义 7.3.1 设 A 是非空集合，A^2 到 A 的一个映射 $f:A^2 \to A$ 称为 A 的一个二元代数运算，简称二元运算。

由二元运算的概念可以推广到一般 n 元运算。

定义 7.3.2 设 A 是非空集合，n 是正整数，A^n 到 A 的一个映射 $f:A^n \to A$ 称为 A 的一个 n 元运算，简称为 n 元运算。

对于集合 A 的一个 n 元运算 f，若 $\langle a_1,a_2,\cdots,a_n\rangle \in A^n$，在 f 的作用下的象是 C，即 $f:\langle a_1,a_2,\cdots,a_n\rangle \to C$，且记为 $C = o(a_1,a_2,\cdots,a_n)$，当 $n=2$ 时，常记作 $a = a_1\, o\, a_2$。

例 7.3.1 设 N 是非负整数集，N^2 到 N 的映射规定为 $f:\langle i,j\rangle \to i+j$，则 f 是 A 上的一个二元运算，其中 $i \circ j = i+j$。

定义 7.3.3 设 A 是一个非空集合，$f_1, f_2, \cdots, f_s$ 分别是 A 的 $k_1, k_2, \cdots, k_s$ 元运算，k_i 是正整数，$i=1,2,\cdots,s$。称集合 A 和运算 $f_1, f_2, \cdots, f_s$ 所组成的系统为一个代数系统（或一个代数结构），简称为一个代数，用记号$(A, f_1, f_2, \cdots, f_s)$表示。当 A 是有限集合时，也称该系统是有限代数系统。

例 7.3.2 最简单的一个代数系统是(N,S)，其中 N 是自然数集，S 是由贝安诺后继函数定义的 N 上的一元运算，即 $S(n) = n+1$ 。

例 7.3.3 $(R,+,\cdot)$是一个代数系统，其中 R 是实数集，$+$和$\cdot$是通常的加法和乘法运算。

例 7.3.4 设 A 是一个非空集合，2^A 是它的幂集，在 2^A 中定义二元运算$+$和$\cdot$为

$$B + C = B \cup C, \quad B \cdot C = B \cap C。$$

对于任意 $B, C \in 2^A$，$(2^A,+,\cdot)$是一个代数系统。

例 7.3.5 设 $M_n(R)$是全体 $n \times n$ 实矩阵的集合，$M_n(R)$ 中的二元运算$\cdot$是通常的矩阵乘法，则$(M_n(R),\cdot)$是一个代数系统。

例 7.3.6 设 $A = \{a_1, a_2, \cdots, a_n\}$，$A$ 中的二元运算$\cdot$定义如下：

对任意的 $a_i, a_j \in A$，$a_i \cdot a_j = a_i$，则$(A,\cdot)$是一个代数系统。

由代数系统的定义可知，一个代数系统是由一个非空集合和该集合上的若干个代数运算结合而成的。集合和代数运算是一个代数系统的两要素，缺一不可。

当然，广义的说，一个代数系统可以由若干个集合和这些集合中的一个或多个 n 元运算所构成，不过在本书中我们主要讨论一个集合，同时重点讨论由一个或两个二元运算构成的代数系统。

在代数系统$(X,\cdot)$中，如果对所有的 $x_i, x_j \in X$，

$$x_i \cdot x_j = x_j \cdot x_i$$

成立，则称$(X,\cdot)$对于二元运算$\cdot$适合交换律。

如果对任意 $x_i, x_j, x_k \in X$，

$$(x_i \cdot x_j) \cdot x_k = x_i \cdot (x_j \cdot x_k)$$

成立，则称代数系统$(X,\cdot)$对于$\cdot$适合结合律。

不难看出，例 7.3.3 和例 7.3.4 适合结合律和交换律，例 7.3.5 和例 7.3.6 适合结合律，却不服从交换律。一般说来，一个代数运算并不一定适合交换律，也不一定满足结合律，因此代数运算是一种概念更一般的运算。

如果$(X,\cdot)$对于$\cdot$适合结合律，那么也一定适合多个元素的广义结合律，可以在表达式中省略括号，例如

$$(((x_1 \cdot x_2) \cdot x_3) \cdots) \cdot x_n = x_1 \cdot x_2 \cdot x_3 \cdot \cdots \cdot x_n。$$

这样，可以令 $x^n = \underbrace{x \cdot x \cdot \cdots \cdot x}_{n}$，并称为 x 的 n 次幂，亦即 x^n 可定义成

$$x^1 = x,$$
$$x^n = x^{n-1} \cdot x, \quad n = 2,3,\cdots。$$

定理 7.3.1 若$(X,\cdot)$对二元运算·适合结合律，则对于任何正整数 m 和 n，有

1. $x^m \cdot x^n = x^{m+n}$。

2. $(x^m)^n = x^{mn}$。

证明：对 n 进行归纳。当 $n=1$ 时，$x^m \cdot x = x^{m+1}$，$(x^m)^1 = x^m$，命题正确；对所有的 $n \leqslant k$，假定 $x^m \cdot x^k = x^{m+k}$，$(x^m)^k = x^{mk}$成立，那么当 $n=k+1$ 时，

$$x^m \cdot x^{k+1} = x^m \cdot (x^k \cdot x) = (x^m \cdot x^k) \cdot x = x^{m+k} \cdot x = x^{m+(k+1)}。$$

$$(x^m)^{k+1} = (x^m)^k \cdot (x^m)^1 = x^{mk} \cdot x^m = x^{mk+m} = x^{m(k+1)}。$$

因此定理得证。

定义 7.3.4 给定一个代数系统 $V = (X,\cdot)$，如果存在一个元素 e_L(或者 e_R)$\in X$，使得对于任意元素 $x \in X$，有 $e_L \cdot x = x$(或 $x \cdot e_R = x$)，称 e_L(或 e_R)是 X 上关于运算·的一个左(或右)单位元。若 e 既是左单位元又是右单位元，则称之为单位元。

例如，在例 7.3.1 中 0 是单位元，例 7.3.5 中有单位元 I(n 阶单位矩阵)，例 7.3.6 中的每个元素都是右单位元，但没有左单位元。

定理 7.3.2 若代数系统 $V = (X,\cdot)$有左单位元 e_L，又有右单位元 e_R，则 $e = e_L = e_R$ 是 X 的唯一的单位元。

证明：因为 e_L 是左单位元，故 $e_L \cdot e_R = e_R$，又因为 e_R 是右单位元，故 $e_L \cdot e_R = e_L$，所以 $e_L = e_R = e$ 是单位元，设 e'是 X 中的任一单位元，则 $e' = e' \cdot e = e$，因此 e 是唯一的单位元。

定义 7.3.5 设 $V = (X,\cdot)$是有单位元 e 的代数系统，对于 $x \in X$，若存在一个元素 x'，使得 $x' \cdot x = e$，则称 x 是左可逆的，并称 x'是 x 的一个左逆元；若存在 $x'' \in X$，使得 $x \cdot x'' = e$，则称 x 是右可逆的，并称 x''是 x 的一个右逆元；若 x 既是左可逆又是右可逆的，则说 x 是可逆元。

比如例 7.3.1 中只有 0 是可逆元，例 7.3.5 中的非奇异矩阵都是可逆元。

定理 7.3.3 设代数系统 $V = (X,\cdot)$具有单位元 e，且适合结合律，对于 $x \in X$，x 有左逆元 x'，又有右逆元 x''，则 x 有唯一逆元 $x^{-1} = x' = x''$，并且 $(x^{-1})^{-1} = x$。

证明：因为 $x' \cdot x = e$，$x \cdot x'' = e$，所以

$$x' = x' \cdot e = x' \cdot (x \cdot x'') = (x' \cdot x) \cdot x'' = e \cdot x'' = x''。$$

假定 x 有两个逆元 a,b，则 $x \cdot a = e$，$b \cdot x = e$，于是

$$b = b \cdot e = b \cdot (x \cdot a) = (b \cdot x) \cdot a = e \cdot a = a。$$

因此 x^{-1}是唯一的。又由于 $x^{-1} \in X$ 且有唯一逆元 x，而

$$x^{-1} \cdot (x^{-1})^{-1} = (x^{-1})^{-1} \cdot x^{-1} = e。$$

因此 $(x^{-1})^{-1} = x$。

例 7.3.7 给定代数系统 $V = (Z,+,\times)$，其中 Z 是整数集，$+$和$\times$分别是通常的加法和乘法运算。它们适合结合律和交换律，对任意 $a,b,c \in Z$

$$(a+b)+c = a+(b+c)。$$

$$(a \times b) \times c = a \times (b \times c)。$$

$$a+b = b+a。$$

$$a \times b = b \times a。$$

同时具有单位元

$$a + 0 = 0 + a = a。$$

$$a \times 1 = 1 \times a = a。$$

即 0 对于加法是单位元，1 对于乘法是单位元。

关于逆元，对任意 $a \in Z$，

$$a + (-a) = (-a) + a = 0 。$$

即对于加法，$-a$ 是 a 的逆元；对于乘法，a $(\neq \pm 1)$ 不存在逆元。

7.4 同构与同态

有些代数系统，它们除了元素的名称和运算符号不同以外，在结构上是没有差别的；还有些代数系统，虽然在结构上不完全相同，但也有许多相似之处。

定义 7.4.1 设 $V_1 = (X, o_1, o_2, \cdots, o_r)$ 和 $V_2 = (Y, \bar{o}_1, \bar{o}_2, \cdots, \bar{o}_r)$ 是两个代数系统，若 o_i 和 $\bar{o}_i$ 都是 k_i 元运算，k_i 是正整数，$i = 1, 2, \cdots, r$，则说代数系统 V_1 和 V_2 是同类型的。

例 7.4.1 设 $A = \{a, b\}$，$B = \{0, 1\}$，A 上的二元运算＋和×上二元运算如下表

+	a	b
a	a	b
b	b	a

×	0	1
0	0	1
1	1	0

则代数系统$(A, +)$和$(B, \times)$是同类型的。进一步考察两个运算表，发现若将 A 中的元素 a, b 分别用 0，1 替换，运算符号＋用×替换，就可以得到$(B, \times)$的运算表。这表明只要在 A 和 B 之间建立一个映射 f，其中 $f(a) = 0$，$f(b) = 1$，则对任意 $x, y \in A$，

$$f(x + y) = f(x) \times f(y)$$

成立。这时也说映射 f 是保持运算的。

定义 7.4.2 设$(X, \cdot)$和$(Y, *)$的两个同类型的代数系统，$f: X \to Y$ 是一个双射。如果对任意元 $a, b \in X$，恒有

$$f(a \cdot b) = f(a) * f(b)。$$

则称 f 是$(X, \cdot)$到$(Y, *)$的一个同构映射，并称$(X, \cdot)$与$(Y, *)$同构，用 $X \cong Y$ 表示。

例 7.4.2 $(Z_4, +)$是一个代数系统，其中 $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ 是整数模 4 同余所确定的等价类集合，Z_4 上的运算＋定义如下：

$$\bar{i} + \bar{j} = \overline{i + j} \pmod 4，$$

其运算表是：

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

另外设 $Y = \{a,b,c,d\}$，并定义 Y 上的运算 $\cdot$ 如下：

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$(Y,\cdot)$与$(Z_4,+)$是同类型的代数系统。现定义 $f:Z_4\to Y$ 如下：

$$f:\bar{0}\to a,\bar{1}\to b,\bar{2}\to c,\bar{3}\to d。$$

可以判断 f 是同构映射，因此 $Z_4\cong Y$。

注意，定义 7.4.2 中的 f 是双射，如果 f 是 X 到 Y 的映射，就相应得到同态的定义。

定义 7.4.3 设$(X,\cdot)$和$(Y,*)$是两个同类型的代数系统，f 是 X 到 Y 的一个映射。如果对任意的 $a,b\in X$，都有 $f(a\cdot b) = f(a) * f(b)$，则称 f 是$(X,\cdot)$到$(Y,*)$的一个同态映射，简称同态。

根据定义可知 $f(X)\subseteq Y$，例如图 7.7 表示一个同态 f。其中 $f(x_1)=f(x_3)=y_1$，$f(x_2)=y_2$，$y_1 * y_2=y_3$。

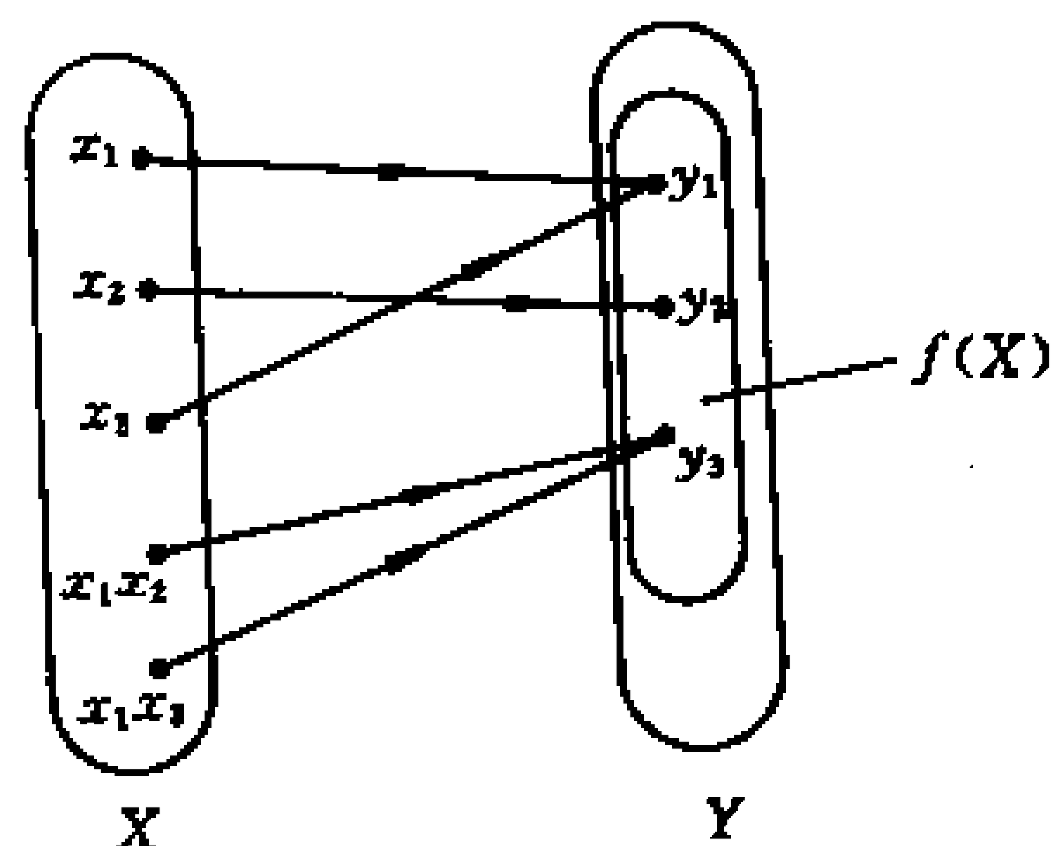


图 7.7

例 7.4.3 一个代数系统 $V_1=(Z,+,\times)$，其中 Z 是整数集合，$+$和$\times$分别一般的加法和乘法运算；另一个代数系统 $V_2=(Z_m,+_m,\times_m)$中，$Z_m=\{\bar{0},\bar{1},\cdots,\overline{m-1}\}$，$+_m$ 和$\times_m$ 分别是模 m 的加法和乘法运算，即

$$\bar{x}_1 +_m \bar{x}_2=\overline{x_1 + x_2}。$$
$$\bar{x}_1 \times_m \bar{x}_2=\overline{x_1 \times x_2}。$$

这样对任意整数 i 和正整数 m，可定义映射 $f:Z\to Z_m$如下

$$f(i) = \bar{i},$$

则 f 是 V_1 到 V_2 的一个同态。因为对任意的 $i,j\in Z$，恒有

$$f(i + j)= \overline{(i + j)} = \bar{i} +_m\bar{j} = f(i) +_m f(j)。$$
$$f(i \times j)= \overline{(i \times j)} = \bar{i} \times_m\bar{j} = f(i) \times_m f(j)。$$

如果 $f:X\to Y$ 是从$(X,\cdot)$到$(Y,*)$的一个同态，那么$(f(X),*)$ 是不是一个代数系统呢？为回答这一问题，先介绍一个定义。

定义 7.4.4 设$(S,\cdot)$是一个代数系统，R 是 S 的一个非空子集，如果 R 在运算 $\cdot$ 下是封闭的，则称$(R,\cdot)$是$(S,\cdot)$的一个子代数系统或子代数。

定理 7.4.1 设映射 $f:X\to Y$ 是从代数系统$(X,\cdot)$到$(Y,*)$ 的一个同态，则$(f(X),*)$是$(Y,*)$的一个子代数，并称它是在 f 作用下$(X,\cdot)$的同态象。

证明：由于 f 是 X 到 Y 的映射，故 $f(X)\subseteq Y$。设任意元 $y_1,y_2\in f(X)$，则一定存在 $x_1,x_2\in X$，使 $f(x_1) = y_1$，$f(x_2) = y_2$。而且 $x_1\cdot x_2= x_3\in X$。因此 $y_1 * y_2= f(x_1) * f(x_2) = f(x_1\cdot x_2) = f(x_3)\in f(X)$，即 $f(X)$对于运算 $*$ 是封闭的。定理得证。

定义 7.4.5 设 $f: X \to Y$ 是从 $(X, \cdot)$ 到 $(Y, *)$ 的一个同态，如果

1. f 是单射，称 f 是单一同态。

2. f 是满射，称 f 是满同态，用 $X \sim Y$ 表示，并称 Y 是 X 的一个同态象。

当然如果 f 是双射，它就是同构。同构是同态的一种更特殊的情况。

例 7.4.4 设 $B = \{0,1\}$，B 上的＋运算由下表给出：

+	0	1
0	0	1
1	1	0

则对 $(Z_4, +_4)$ 和 $(B, +)$ 两个代数系统而言，设映射 $\varphi: Z_4 \to B$ 是由

$$\varphi(x) = \begin{cases} 0, & x = \bar{0}, \bar{2} \text{ 时。} \\ 1, & x = \bar{1}, \bar{3} \text{ 时。} \end{cases}$$

给出，易见 φ 是 $(Z_4, +_4)$ 到 $(B, +)$ 的一个满同态。

定理 7.4.2 给定代数系统 $(X, \cdot)$ 和 $(Y, *)$，其中 $\cdot$ 和 $*$ 都是二元运算。设 $f: X \to Y$ 是 $(X, \cdot)$ 到 $(Y, *)$ 的满同态，则

1. 如果 $\cdot$ 是可交换的或可结合的运算，则 $*$ 也是可交换的或可结合的运算。

2. 若 $(X, \cdot)$ 中运算 $\cdot$ 具有单位元 e，则 $(Y, *)$ 中运算 $*$ 具有单位元 $f(e)$。

3. 对运算 $\cdot$，如果每一个元素 $x \in X$ 都有逆元 x^{-1}，则对运算 $*$，每一个元素 $f(x) \in Y$ 都具有逆元 $f(x^{-1})$。

证明：

1. 因为 $f: X \to Y$ 是满同态，所以能把 Y 中的每个元写成 $f(x)$ 的形式。如果运算 $\cdot$ 是可交换的或可结合的，则对任意 $f(x_1), f(x_2), f(x_3) \in Y$，有

$$\begin{aligned} f(x_1) * f(x_2) &= f(x_1 \cdot x_2) = f(x_2 \cdot x_1) \\ &= f(x_2) * f(x_1)。\\ (f(x_1) * f(x_2)) * f(x_3) &= f(x_1 \cdot x_2) * f(x_3) \\ &= f((x_1 \cdot x_2) \cdot x_3) \\ &= f(x_1 \cdot (x_2 \cdot x_3)) \\ &= f(x_1) * f(x_2 \cdot x_3) \\ &= f(x_1) * (f(x_2) * f(x_3))。\end{aligned}$$

因此运算 $*$ 也是可交换的和可结合的。

2. 对运算 $\cdot$ 来说，设 e 是单位元，$e \in X$，则对任意 $f(x) \in Y$，

$$f(x) * f(e) = f(x \cdot e) = f(x)。$$
$$f(e) * f(x) = f(e \cdot x) = f(x)。$$

因此运算 $*$ 具有单位元 $f(e)$。

3. 同理，设 x 是 X 中的任意元，x^{-1} 是 x 关于运算 $\cdot$ 的逆元，显然 $x^{-1} \in X$，则对任意 $f(x) \in Y$，有

$$f(x) * f(x^{-1}) = f(x \cdot x^{-1}) = f(e)。$$
$$f(x^{-1}) * f(x) = f(x^{-1} \cdot x) = f(e)。$$

因此 $f(x^{-1})$是 $f(x)$ 的逆元。

定理说明代数系统$(X,\cdot)$所适合的一些运算性质，如结合律、交换律、可逆律等，在该系统的任何满同态象中，特别是同构象中都能完整地保持下来。因此如果已经获知某代数系统的运算性质，同时证明了另一系统 Y 是它的同态象，就能立刻获知系统 Y 同样具有这些运算性质，而无需逐一论证。

以下再给出自同态和自同构的定义。

定义 7.4.6 代数系统$(X,\cdot)$上的同态映射 $f:X\to X$ 称为自同态，若 f 是同构映射，则称之为自同构。

例 7.4.5 已知代数系统 $V=(Z^+,+)$，Z^+是正整数集合，+是普通加法运算。设φ是恒等映射，即对任意 $a\in Z^+$，$\varphi(a)=a$，显然φ是一个双射。这样对于任意的 b、$c\in Z^+$，有

$$\varphi(b+c)=b+c=\varphi(b)+\varphi(c)。$$

因此φ是代数系统 V 的一个自同构。

例 7.4.6 设 $A=\{1,2,3\}$，代数运算 $*$ 定义如下：

*	1	2	3
1	1	2	1
2	1	2	2
3	1	2	3

那么，$f:1\to 2,2\to 1,3\to 3$ 是$(A,*)$上的自同构。

习 题 七

1. 设 $f:A\to B$，其中$|A|=m$，$|B|=n$，当$(a)\ m<n$，$(b)\ m=n$，$(c)\ m>n$ 时，分别有多少个不同的单射和双射？

2. 证明若 $f:A\to B$，$g:B\to C$，则

   (a) 当 f、g 都是单射时，gf 也是单射。

   (b) 当 f、g 都是满射时，gf 也是满射。

   (c) 当 f、g 都是双射时，gf 也是双射。

3. 设 A、B 是两个有限集，且$|A|=|B|$，证明 $f:A\to B$ 是单射当且仅当 f 是满射。

4. 令 $A=\{1,2,\cdots\}$，f，g 是 A 上的两个映射，是否可能 $gf=I_A$ 而 $fg\neq I_A$？试举一例说明。如果 f 是双射，结果又是怎样呢？

5. 令 $f:S\to T$，且 A、B 是 S 的子集。证明 $f(A\cup B)=f(A)\cup f(B)$，$f(A\cap B)$ $f(A)\cap f(B)$。并举例说明之。

6. 已知 $\sim$ 是 A 上的一个等价关系，$A/\sim$ 是 A 的子集还是 2^A 的子集？

7. 证明自然数集上的模 m 同余关系是等价关系。

8. 证明若 R 和 S 是集合 A 上的等价关系，则 $R\cap S$ 也是等价关系。

9. 设 $A=\{1,2,3,4\}$，在 2^A 中规定二元关系 $\sim$，$S\sim T \Longleftrightarrow S$、$T$ 含有相同的

元素个数，证明 ~ 是一个等价关系，写出商集 $2^A/\sim$ 。

10. 令 N 是自然数集，$N^2 = N\times N$，在 N^2 上定义 $(a,b)\sim(c,d)$，若 $a+d = b+c$，证明 ~ 是等价关系。

11. 代数系统 $V = (R, *)$中，R 是实数集，二元运算 $*$ 分别定义如下：

(a) $a_1 * a_2 = |a_1 - a_2|$。

(b) $a_1 * a_2 = \frac{1}{2}(a_1 + a_2)$。

(c) $a_1 * a_2 = a_1/a_2$。

对每一种情况，$(R, *)$ 是否可结合或可交换？是否含有单位元？如果有，R 中的每个元素是否都是可逆的？

12. 设 $K = \{e, a, b, c\}$ 定义二元运算 · 如下：

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$(K, \cdot)$是否可结合的？有无单位元？每一个元是否可逆？

13. 设代数系统 $V = (X, \cdot)$具有单位元 e，且适合结合律，若 $a,b\in X$ 且可逆，证明 $a\cdot b$ 也是可逆的，并且 $(a\cdot b)^{-1} = b^{-1}\cdot a^{-1}$。

14. 两个代数系统$(N, *)$和$(\{0,1\}, *)$，其中 N 是自然数集，$*$ 是一般的乘法运算，给定映射 $f: N\to\{0,1\}$，其中

$$f(n) = \begin{cases} 1, & \text{若 } n = 2^k (k = 0,1,2,\cdots)。\\ 0, & \text{其它。} \end{cases}$$

试证 f 是$(N, *)$到$(\{0,1\}, *)$的一个同态。

15. 已知代数系统$(S, *)$和$(P, \cdot)$，其中 $S = \{a,b,c\}$，$P = \{1,2,3\}$，二元运算分别定义为：

·	a	b	c
a	a	b	c
b	b	b	c
c	c	b	c

·	1	2	3
1	1	2	1
2	1	2	2
3	1	2	3

试证它们是同构的。

16. 若 $f: A\to B$ 是代数系统$(A, \cdot)$到$(B, *)$的一个同态，而$(A_1, \cdot)$是$(A, \cdot)$的一个子代数，证明 A_1 在 f 下的象是$(B, *)$的一个子代数。

第八章　群

代数系统中最简单的是只具有一个二元运算的系统，本章将要介绍的半群、幺群和群，都是这样的代数系统。群是抽象代数的重要分支。在许多自然科学，包括计算机科学中都得到了广泛的应用，比如在形式语言、自动机理论以及编码理论中都使用了半群、幺群和群的概念。

8.1　半　群

由代数系统的定义可知，其二元运算一定是封闭的。通过进一步观察可以发现，有些代数系统中的二元运算服从结合律，这类代数系统称为半群。

例 8.1.1　代数系统$(Z^+,+)$中，Z^+是正整数的集合，$+$是普通的加法运算，则对任意的 $a,b,c\in Z^+$，$(a+b)+c=a+(b+c)\in Z^+$。

例 8.1.2　设 A 是一个非空集，对任意的 $a,b\in A$，规定 $a\cdot b=b$，则$\cdot$是 A 上的一个二元运算，并且$(a\cdot b)\cdot c=b\cdot c=c=a\cdot c=a\cdot(b\cdot c)$，即运算$\cdot$适合结合律。

例 8.1.3　$(R^*,\div)$是一个代数系统，其中 R^*是非零实数集，$\div$是除法运算，任取 $a,b,c\in R^*$，$a\div(b\div c)\neq(a\div b)\div c$，它不满足结合律。

例 8.1.4　设 $S=\{1,2\}$，S 到自身的变换集合 $M(S)$包含以下 4 个变换：

$$\alpha=\begin{bmatrix}1&2\\1&2\end{bmatrix}\quad\beta=\begin{bmatrix}1&2\\2&1\end{bmatrix}\quad\gamma=\begin{bmatrix}1&2\\1&1\end{bmatrix}\quad\sigma=\begin{bmatrix}1&2\\2&2\end{bmatrix}$$

其中 α 是恒等变换。可以验证 $M(S)$中的乘法表如下：

$\cdot$	α	β	γ	σ
α	α	β	γ	σ
β	β	α	σ	γ
γ	γ	γ	γ	γ
σ	σ	σ	σ	σ

$\cdot$满足结合律。例如$(\beta\cdot\sigma)\cdot\gamma=\gamma\cdot\gamma=\gamma$，$\beta\cdot(\sigma\cdot\gamma)=\beta\cdot\sigma=\gamma$。

定义 8.1.1　设 S 是非空集合，$\cdot$是 S 上的一个二元运算，如果$\cdot$满足结合律，则代数系统$(S,\cdot)$称为半群。

换句话说，如果对于任意的 $a,b,c\in S$，若$(a\cdot b)\cdot c=a\cdot(b\cdot c)$ 成立，则称$(S,\cdot)$为半群。

例 8.1.1 和例 8.1.2 是半群，例 8.1.3 不是半群。例 8.1.4 是半群，进一步观察发现 α 是其中的单位元。对于有单位元的半群，称之为含幺半群。

定义 8.1.2　若半群$(M,\cdot)$中有单位元 e 存在，则称$(M,\cdot)$是一个含幺半群或简称幺群。

幺群有时也用三元组$(M,\cdot,e)$表示，M 表示非空集合，$\cdot$ 是 M 上的二元运算，且适合结合律，e 表示 M 中关于运算 $\cdot$ 的单位元，即 $a\cdot e=e\cdot a=a$。为方便起见，可以直接称 M 为幺群，同时经常用 ab 表示 $a\cdot b$，并称为 a 与 b 的乘积。

例 8.1.5 $(N,+,0)$是幺群，其中 N 是非负整数集。

例 8.1.6 $(N,\times,1)$是幺群。

例 8.1.7 $(Z,+,0)$和$(Z,\times,1)$是幺群，其中 Z 是整数集。

例 8.1.8 设 $M=\{1,2,\cdots,10\}$，MAX 和 MIN 都是 M 上的二元运算，M 对这两个运算都是封闭的，而且 $MAX(a,MAX(b,c))=MAX(MAX(a,b),c)$，$MIN(a,MIN(b,c))=MIN(MIN(a,b),c)$，因此$(M,MAX,1)$和$(M,MIN,10)$都是幺群。

例 8.1.9 设 2^A 是 A 的全部子集的集合，则$(2^A,\cup,\Phi)$和$(2^A,\cap,A)$都是幺群。

例 8.1.10 设$(Z)_n$ 表示一切元素为整数的 n 阶方阵的集合，则$(Z)_n$ 对于矩阵乘法作成一个幺群，其中单位元是 n 阶单位矩阵 I。

例 8.1.11 设 $Z_m=\{\bar{0},\bar{1},\cdots,\overline{m-1}\}$是模 m 同余的等价类集合，$\cdot$ 是 Z_m 上的模 m 加法运算，它有单位元 $\bar{0}$，因此$(Z_m,\cdot,\bar{0})$是一个幺群。

定义 8.1.3 设$(M,\cdot,e)$是一个幺群，若 $\cdot$ 适合交换律，则称 M 是交换幺群。

例 8.1.5 到 8.1.11 中，除 8.1.10 以外都是交换幺群。由于矩阵乘法不适合交换律，因此例 8.1.10 不是交换幺群。

令 $a_1,a_2,\cdots,a_n$是幺群 M 中的一个元素序列，如果不改变元素的次序，那么可以确定多种二元运算的合成，比如 $n=4$，可以有

$$((a_1a_2)a_3)a_4,(a_1(a_2a_3))a_4,(a_1a_2)(a_3a_4),\ a_1((a_2a_3)a_4),a_1(a_2(a_3a_4))$$

不失一般性，可以把该序列分为两个子序列 $a_1,a_2,\cdots,a_m$ 和 $a_{m+1},\cdots,a_n(1\leqslant m<n)$来得到 $a_1,a_2,\cdots,a_n$ 的乘积，假定我们已经分别知道 $a_1,\cdots,a_m$，和 $a_{m+1},\cdots,a_n$ 的乘积，那么它们之间运算合成的结果就是次序为 $a_1,\cdots,a_n$ 的 M 中的一个元素。由于二元运算适合结合律，所以当 m 的取值范围在 1 和 $n-1$ 之间时，使用归纳法可以证明这些结果都是相同的。

当 $n=2$ 时，结论为真。

设小于 n 时结论为真，当等于 n 时，设最后一次计算是在 $\prod_1^m a_i$ 和 $\prod_1^{n-m} a_{m+j}$ 之间进行的，因此

$$\begin{aligned}\prod_1^m a_i\prod_1^{n-m} a_{m+j} &= \prod_1^m a_i\Big(\Big(\prod_1^{n-m-1} a_{m+j}\Big)a_n\Big)\\ &= \Big(\prod_1^m a_i\prod_1^{n-m-1} a_{m+j}\Big)a_n\\ &= \prod_1^{n-1} a_i\cdot a_n=\prod_1^n a_i。\end{aligned}$$

于是我们有

定理 8.1.1 如果二元运算 $\cdot$ 适合结合律，那么也适合广义结合律。

如果所有的 $a_i=a$，可以记 $a_1a_2\cdots a_n$ 为 a^n，并称为 a 的 n 次幂。由定理 8.1.1 显见

$$a^m a^n = a^{m+n}, (a^m)^n = a^{mn}, \ m,n \in N$$

其中定义 $a^0=e$，即 M 中的单位元。

如果 a 是 M 中的一个可逆元，那么一定有 $a^{-1}\in M$，于是 $a^{-1}a^{-1}\cdots a^{-1}$（$n$ 个）可以表示为 $(a^{-1})^n=a^{-n}$，当然 $a^{-n}=(a^n)^{-1}$ 也是成立的，因此上式中的 m,n 在整数范围内取值都是成立的。

定义 8.1.4 设 $(M,\cdot,e)$ 是一个幺群，若存在一个元素 $g\in M$，使得对任意 $a\in M$，a 都可以写成 g 的方幂形式，即 $a=g^m$（m 是非负整数），则称 $(M,\cdot,e)$ 是一个循环幺群，且并称 g 是 M 的一个生成元。

例 8.1.11 中，令 $g=\bar{1}$，则 $\bar{2}=\bar{1}\cdot\bar{1}=(\bar{1})^2,\bar{0}=(\bar{1})^0,\cdots$，因此 $(Z_m,\cdot,\bar{0})$ 是循环幺群，$\bar{1}$ 是一个生成元。

定理 8.1.2 循环幺群是可交换幺群。

证明：设 g 是循环幺群中的一个生成元，则对任意 $a,b\in M$，有 $a=g^m,b=g^n,(m,n\geqslant 0)$，由于二元运算适合交换律，因此

$$ab=g^m g^n=g^{m+n}=g^{n+m}=g^n g^m=ba \ 。$$

所以循环幺群是可交换的。

以下再引入子半群和子幺群的概念。

定义 8.1.5 设 $(S,\cdot)$ 是一个半群，$T\subseteq S$，在运算 $\cdot$ 的作用下如果 T 是封闭的，则称 $(T,\cdot)$ 是 $(S,\cdot)$ 的子半群。

定义 8.1.6 设 $(M,\cdot,e)$ 是一个幺群，$T\subseteq M$，在运算 $\cdot$ 的作用下如果 T 是封闭的，且 $e\in T$，则称 $(T,\cdot,e)$ 是 $(M,\cdot,e)$ 的子幺群。

比如在例 8.1.1 的半群 $(Z^+,+)$ 中，$m\in Z^+$，设 T 是 m 的正整数倍的集合，则 $(T,+)$ 是 $(Z^+,+)$ 的子半群；又如幺群 $(N,\times,1)$ 中，$m\in N$，设 T 是 m 的非负整数倍的集合，如果 $m\neq 1$，则 T 中不含元素 1，故 $(T,\times)$ 不是 N 的子幺群，而是其子半群，但当 $m=1$ 时，$T=N$，因此 $(T,\cdot,1)$ 是 N 的子幺群。

例 8.1.12 设 $(M,\cdot,e)$ 是一个幺群，则 $(\{e\},\cdot,e)$ 和 $(M,\cdot,e)$ 都是 M 的子幺群，称为平凡子幺群。M 中除了自身以外的子幺群称为真子幺群。

例 8.1.13 设 $\Sigma=\{a,b,c\}$，Σ^+ 是非空字符串的集合，$\Sigma^*=\phi\cup\Sigma^+$，$\cdot$ 是字符的联接运算，则 $(\Sigma^+,\cdot)$ 是一个半群，$(\Sigma^*,\cdot,\phi)$ 是幺群。若 Σ' 是 Σ^* 中所有不含字母 a 的字符串集合，则 $(\Sigma',\cdot)$ 是 Σ^+ 的子半群，$(\Sigma'\cup\phi,\cdot,\phi)$ 是 Σ^* 的子幺群。

例 8.1.14 设 $(A)_n$ 表示一切元素为有理数的 n 阶方阵集合，则集合 $(A)_n$ 对于矩阵乘法作成一个幺群，其中单位矩阵 I 是单位元。例 8.1.10 的 $(Z)_n$ 是它的一个子幺群。令 $T=\{(a_{ij})\in(Z)_n \mid 若\ i\leqslant j\ ，则\ a_{ij}=0\}$，即 T 是元素为整数的下三角矩阵的集合，则 T 对于矩阵乘法封闭。但由于 $I\notin T$，所以 T 是 $(Z)_n$ 的一个子半群，而不是子幺群。

由于幺群 M 中的单位元 e 是唯一的，因此仅当其子半群 T 中含有 e 时，T 才是子幺群。

将一般代数系统的同态、同构概念应用在半群和幺群上，可以得到如下定义：

定义 8.1.7 设 $(A,\cdot)$、$(B,*)$ 是两个半群（幺群），f 是 A 到 B 的一个映射，对于任意 $a,b\in A$，若 $f(a\cdot b)=f(a)*f(b)$ 成立，则称 f 是从半群（幺群）A 到半群（幺群）B

的同态映射，简称同态。若 f 分别是单射、满射和双射时，分称 f 是单同态、满同态和同构。

例 8.1.15 $(R,+,0)$和$(C^*,\cdot,1)$是两个幺群。其中 R 是实数集，$C*$ 是非 0 复数集，令 $f: \theta \to e^{i\theta}$，则对任意的 $a,b\in R$，有

$$f(a+b)=e^{i(a+b)}=e^{ia+ib}=e^{ia}*e^{ib}=f(a)*f(b)。$$

因此 f 是 R 到 C^* 的同态。

如果 f 是幺群 A 到 B 的同态，那么它不但保持运算，而且一定将 A 中的单位元映射到 B 的单位元，否则即使 f 保持运算，也不称为同态。

例 8.1.16 $(Z,*,1)$ 和 $(\{0\},\cdot,0)$ 是两个幺群，令 $f: a\to 0$，则 f 是 Z 到 $\{0\}$ 的一个映射，同时满足 $f(a\cdot b)=f(a)\cdot f(b)$，因此 f 是一个同态。另外，虽然 $g: a\to 0$ 也是 Z 到 Z 的一个映射，它同样满足 $g(a\cdot b)=g(a)\cdot g(b)$，但是 g 不是 Z 到 Z 的同态，因为 $g(1)=0$，而 0 不是 Z 中的单位元。

定理 8.1.3 设 f 是从代数系统 $(A,\cdot)$ 到 $(B,\cdot *)$ 的满同态，S 是 A 的非空子集。$f(S)$ 表示 S 中的元素在 f 下的象的集合，即 $f(S)=\{f(a)|a\in S\}$，那么

1. 若$(S,\cdot)$是半群，则$(f(S),*)$也是半群。
2. 若$(S,\cdot)$是幺群，则$(f(S),*)$也是幺群。

证明：显然 $f(S)$是非空集合。要证明$(f(S),*)$是半群，只要证明 $f(S)$对运算 $*$ 是封闭的，且 $*$ 在 $f(S)$上适合结合律。对于任意 $a',b',c'\in f(S)$，必有 $a,b,c\in S$，使 $f(a)=a'$，$f(b)=b'$，$f(c)=c'$，由于 f 是同态，因此

$$a'*b'=f(a)*f(b)=f(a\cdot b)。$$

由于 S 是半群，所以 $ab\in S$，即 $f(ab)\in f(S)$，可知 $f(S)$对于运算 $*$ 是封闭的。再者，因为

$$a'*(b'*c')=f(a)*(f(b)*f(c))=f(a)*f(b\cdot c)$$
$$=f(a\cdot b\cdot c)。$$
$$(a'*b')*c'=(f(a)*f(b))*f(c)=f(a\cdot b)*f(c)$$
$$=f((a\cdot b)\cdot c)。$$

由于 S 是半群，易知 $a\cdot(b\cdot c)=(a\cdot b)\cdot c$，因此 $a'*(b'*c')=(a'*b')*c'$，即 $*$ 在 $f(S)$上适合结合律，故$(f(S),*)$是半群。

对第二部分，只需再证明$(f(s),*)$也有单位元。因为$(S,\cdot)$是幺群，故$(S,\cdot)$中有单位元 e，令 $f(e)=e'$，$f(e)\in f(S)$，因此对任意 $a'\in f(S)$。

$$e'*a'=f(e)*f(a)=f(ea)=f(a)=a'。$$
$$a'*e'=f(a)*f(e)=f(ae)=f(a)=a'。$$

所以 e' 是$(f(S),*)$中的单位元，故$(f(S),*)$是幺群。

作为定理 8.1.3 的特例，可以得到以下推论：

推论：设 f 是从半群(幺群)$(A,\cdot)$到代数系统$(B,*)$的满同态，$(S,\cdot)$是$(A,\cdot)$的子半群(子幺群)，则有

1. $(B,*)$是半群(幺群)。
2. $(f(S),*)$是$(B,*)$的子半群(子幺群)。

它说明一个半群或幺群的同态象仍然是半群或幺群。

8.2 群、群的基本性质

定义 8.2.1 设 G 是非空集合，$\cdot$ 是 G 上的二元运算，若代数系统 $(G,\cdot)$ 满足

1. 适合结合律，即对任意的 $a,b,c\in G$，有

$$(ab)c = a(bc)$$

2. 存在单位元，即对任意 $a\in G$，$ae=ea=a$。

3. G 中的元素都是可逆元。即对任意 $a\in G$，都存在 $a^{-1}\in G$，使得

$$a^{-1}a = aa^{-1} = e。$$

则称代数系统 $(G,\cdot)$ 是一个群，或记为 $(G,\cdot,e)$。

为方便起见，常用 G 表示群 $(G,\cdot)$。由定义可知群也必定是幺群。因此也可以将群定义如下：

定义 8.2.2 设 $(G,\cdot,e)$ 是含幺半群，e 是其单位元，如果对任意 $a\in G$，都存在逆元 $a^{-1}\in G$，使得

$$a^{-1}a = aa^{-1} = e$$

成立，则称 G 是一个群。换言之，G 是所有元素都可逆的含幺半群。

定义 8.2.3 若群 G 的二元运算 $\cdot$ 满足交换律，即对任意的 $a,b\in G$，都有 $ab=ba$ 则称 G 是交换群，或阿贝尔(Abel)群。

规定集合 G 的基数就是群 $(G,\cdot)$ 的阶，当阶为某一整数时，称该群是有限群，否则为无限群。

例 8.2.1 $(Q,+,0)$ 是群，其中 Q 是有理数集，对任意元 $a\in Q$，都有 $-a\in Q$，即 $a+(-a)=(-a)+a=0$。

例 8.2.2 $(Q^*,\cdot,1)$，其中 Q^* 是非 0 有理数集，对任意 $a\in Q^*$，都有 $\frac{1}{a}\in Q^*$，使 $a\cdot\frac{1}{a}=\frac{1}{a}\cdot a=1$，因此 $(Q^*,\cdot,1)$ 是无限群。

例 8.2.3 $(Z_n,+,\bar{0})$ 是一个群，称为剩余类加群，对 Z_n 中的任意元 $\bar{i}$，都有逆元 $\overline{n-i}$。

例 8.2.4 设 M 是平面上关于原点 O 的旋转的集合，旋转的合成运算如常，旋转一个角度 θ 可以用解析方法表示成从 (x,y) 到 (x',y') 的一个映射 ρ_θ，其中

$$x' = x\cos\theta - y\sin\theta,\ y' = x\sin\theta + y\cos\theta。$$

恒等映射是 $\rho_{\theta=0}$，对每一个旋转角度 θ 所对应的映射 ρ_θ，都有它的逆 $\rho_{-\theta}$，因此 M 是一个群。

例 8.2.5 $(R^{(3)},+,0)$ 中，$R^{(3)}$ 是三维欧几里得空间，$+$ 是通常的向量加法运算，其中 $0=(0,0,0)$。对于任意 $(x,y,z)\in R^{(3)}$，都有 $(-x,-y,-z)\in R^{(3)}$，使得 $(x,y,z)+(-x,-y,-z)=(-x,-y,-z)+(x,y,z)=(0,0,0)$，因此 $(R^{(3)},+,0)$ 是群。

有时 M 上二元运算的结果并非很有规律性，这时我们经常依据乘法表判断 M 是否为一个代数系统，如果是，还可以判断它是否为半群、幺群，还是群。

例 8.2.6 设 $M=\{a,b,c\}$，M 上的运算·的乘法表如下：

·	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

试对$(M,\ \cdot)$加以判断。

首先·的确是 M 上的二元运算，其次考察结合律是否成立。从表中可见，对任意 $x\in M$，$xa=ax=x$，所以 x、y、z 中只要有一个元是 a，它必满足结合律，若 x，y，z 是 b 和 c 时，只有

$$b\,b\,b, b\,b\,c, b\,c\,b, b\,c\,c, c\,b\,b, c\,b\,c, c\,c\,b, c\,c\,c,$$

8 种情况，经一一考察，它们也都适合结合律。比如$(bc)c=ac=c$，$b(cc)=bb=c$。因此$(M,\cdot)$是半群，同时因为 a 是单位元，所以$(M,\cdot)$是幺群。

再次，由于 $aa=a$，$bc=cb=a$，所以 $a^{-1}=a$，$b^{-1}=c$，$c^{-1}=b$，即每一个元都有逆元，故$(M,\cdot)$是一个群，而且是阿贝尔群。

例 8.2.7 设 $K_4=\{e,a,b,c\}$，K_4中的乘法表如下：

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

可以验证该运算适合结合律，e 是单位元，对任意 $x\in K_4$，$x^{-1}=x$，所以$(K_4,\cdot)$是群，而且是交换群，称之为 Klein 四元群。

如前所述，如果幺群 M 中的所有元都可逆，则 M 是群。但是有的幺群 M 中只有一部分元素可逆，那么 M 中所有可逆元构成的子集 G 是不是一个群呢？回答是肯定的。因为 $e\in M$，$e\cdot e=e$，所以 e 是可逆元，即 G 是非空集，设任意的 $x,y\in G$，有

$$\begin{aligned}(xy)(y^{-1}x^{-1})&=x(y(y^{-1}x^{-1}))=x((yy^{-1})x^{-1})\\&=x(ex^{-1})=xx^{-1}=e。\\(y^{-1}x^{-1})(xy)&=y^{-1}(x^{-1}(xy))=y^{-1}((x^{-1}x)y)\\&=y^{-1}(ey)=y^{-1}y=e。\end{aligned}$$

因此 $xy\in G$，故 G 关于二元运算是封闭的。

同时也说明若 $a\in G$，则 $a^{-1}\in G$，因此 G 是一个群。

例 8.2.8 $((R_n,\cdot,I)$中，(R) 是所有 $n\times n$ 阶的实矩阵的集合，则$(R)_n$ 是幺群；设 G 是全体 $n\times n$ 阶实可逆矩阵的集合，则 G 是$(R)_n$ 的子集，且构成群。

例 8.2.9 例 8.1.4 中 $M(S)$是一个幺群，它有单位元——恒等变换 α。但不是群。因为 γ 和 δ 没有逆元。但是令 $G=\{\alpha,\beta\}$，则 G 构成群。

由于群是特殊的幺群，所以它有幺群的一切性质。

定理 8.2.1 设 G 是一个群，则

1. G 中的单位元唯一。

2. G 中每个元素都有唯一的逆元。

3. 指数律成立，即对于任意 $a \in G$，设 m, n 是任意整数，有

$$a^m a^n = a^{m+n}, \ (a^m)^n = a^{mn}。$$

4. 若 $ab = ba$，则 $(ab)^n = a^n b^n$

定理 8.2.2 设半群 $(G, \cdot)$ 有一个左单位元 e，且对每一个元 $a \in G$，都有左逆元 $a^{-1} \in G$，使 $a^{-1}a = e$ 成立，则 G 是群。

证明：因为

$$\begin{aligned} ae = eae &= ((a^{-1})^{-1}a^{-1})a(a^{-1}a) = (a^{-1})^{-1}(a^{-1}a)(a^{-1}a) \\ &= (a^{-1})^{-1}(ea^{-1})a = ((a^{-1})^{-1}a^{-1})a = ea = a, \end{aligned}$$

所以 e 也是右单位元。同理可证 a^{-1} 也是 a 的右逆元，设 a' 是 a^{-1} 的左逆元，于是有

$$\begin{aligned} aa^{-1} = eaa^{-1} &= (a'a^{-1})aa^{-1} = a'(a^{-1}a)a^{-1} \\ &= (a'e)a^{-1} = a'a^{-1} = e。 \end{aligned}$$

因此 G 是群。

定理 8.2.3 设 $(G, \cdot)$ 是半群，如果对 G 中任意两个元素 a, b，方程 $ax = b$ 和 $ya = b$ 在 G 中都有解，则 G 是一个群。

证明：因为 $ya = b$，且 b 任意，所以 $ya = a$ 在 G 中有解，设 e 是 $ya = a$ 的一个解。对方程 $ax = b$，设 x 是其中的一个解，那么对任意的 b，

$$eb = e(ax') = (ea)x' = ax' = b \ 。$$

所以 e 是左单位元；再者因为对任意的 $a \in G$，$ya = e$ 有解 y'，所以 y' 是 a 的左逆元。由定理 8.2.2，G 是群。

如果 $(G, \cdot, e)$ 是一个群，由于每个元都有逆元，所以左、右消去律对于群的运算是成立的。也就是说，对任意的 $a, b, c \in G$，

$$ab = ac \Rightarrow b = c \ 。$$

$$ba = ca \Rightarrow b = c \ 。$$

这是因为

由 $ab = ac$ 两边左乘 a^{-1} 得 $b = c$. 类似可证第二式。

定理 8.2.4 设 G 是一个群，对 G 中的任意元素 a, b 恒有：

$$(a^{-1})^{-1} = a, \ (ab)^{-1} = b^{-1}a^{-1}。$$

证明：$\because a^{-1}a = e$，

$\therefore (a^{-1})^{-1} = a$。

$\because (ab)b^{-1}a^{-1} = e$，

$\therefore (ab)^{-1} = b^{-1}a^{-1}$。

设 a 是有限群 G 中的一个非单位元，由消去律，一定有 $a^2 \neq a$，即 a^2 是 G 中的另一个元素，因此，$a, a^2, \cdots, a^{k-1}, a^k = e$ 是 G 中不同的元素，其中 k 是满足 $a^k = e$ 的最小正整数。

定义 8.2.4 设 a 是 G 中的一个元素，若有正整数 k 存在，使 $a^k = e$，则满足 $a^k = e$ 的最小正整数 k 称为元素 a 的阶（或周期），记为 $O\langle a \rangle$，并称 a 是有限阶元素。

比如在 $(Z_{10}, +, \bar{0})$ 中，元素 $(\bar{1})^{10} = \bar{0}$，所以 $O\langle \bar{1} \rangle = 10$，虽然 $(\bar{2})^{10} = \bar{0}$，但 $(\bar{2})^5$ 也为 $\bar{0}$，因

此 $O\langle\bar{2}\rangle=5$。

定理 8.2.5 设 a 是群 G 中的一个 r 阶元素，k 是正整数，则

1. $a^k=e$，当且仅当 $r|k$。

2. $O\langle a\rangle=O\langle a^{-1}\rangle$。

3. $r\leqslant|G|$。

证明：先证第一部分，充分性，因为 $r|k$，所以存在整数 m，使 $k=rm$，于是

$$a^k=a^{rm}=(a^r)^m=e^m=e\ 。$$

必要性。若 $a^k=e$，由带余除法一定存在整数 p,q，使 $k=pr+q$，$(0\leqslant q<r)$，于是 $a^k=a^{pr+q}=a^{pr}a^q=(a^r)^pa^q=a^q=e$，因为 r 是 a 的阶，所以 $q=0$，故 $r|k$。

再证第二部分，设 $O(a)=r,O(a^{-1})=r'$，由定理 8.2.1 中 3，$(a^{-1})^r=(a^r)^{-1}=e$，$\therefore r'|r$，类似可证 $r|r'$，$\therefore r=r'$。

最后，设 $e=a^0,a,\cdots,a^{r-1}$ 中如果有两个元素是相同的，比如 $a^i=a^j$ 其中 $0\leqslant i<j\leqslant r$，则有 $a^{j-i}=e$，即 $0<j-i<r$，与 a 的阶是 r 相矛盾。因此 $e,a,\cdots,a^{r-1}$ 是 G 中 r 个不同的元素，故 $r\leqslant|G|$。

上一节中曾经介绍过子半群和子幺群，对于群，也相应有子群的概念。

定义 8.2.5 设 H 是群 G 的一个非空子集，若 H 对于 G 的运算仍然构成群，则称 H 是 G 的一个子群，记为 $H\leqslant G$。

根据定义，$G\leqslant G$、$\{e\}\leqslant G$，它们称为 G 的平凡子群，若 G 的子群 $H\neq G$，则称 H 是 G 的真子群，可用 $H<G$ 表之。

例 8.2.10 $(Z,+,0)$ 是一个群，设 T 是正整数 m 整倍数的集合，则 $(T,+,0)$ 是 $(Z,+,0)$ 的一个子群。

例 8.2.11 设 G 是全体 $n\times n$ 阶实可逆矩阵的集合，它对矩阵乘法构成群。令 H 是行列式值为 1 的矩阵集合，则 $H<G$，即 H 是 G 的一个子群。

作为群，子群一定具有群的性质；作为某个群 G 的子群，它应该与 G 有一定的联系。

定理 8.2.6 H 是 G 的子群的充要条件是：

1. H 对 G 的乘法运算是封闭的，即对任意的 $a,b\in H$，都有 $ab\in H$。

2. H 中有单位元 e'，且 $e'=e$。

3. 对任意的 $a\in H$，都有 $a^{-1}\in H$，且 a^{-1} 是 a 在 G 中的逆元。

证明：由子群和群的定义可知 H 对 G 的运算是封闭的，且有单位元 e'，对任意 $a\in H$，都有 $a^{-1}\in H$。因为在 G 中，$e'e=e'$，在 H 中，$e'e'=e'$，所以 $e'e=e'e'$。由消去律得到 $e'=e$。再设 a 在 H 中的逆元是 a'，在 G 中的逆元是 a^{-1}，则 $aa^{-1}=e=e'=aa'$，故 $a^{-1}=a'$，这就证明了必要性，充分性是显然的。定理得证。

我们可以将定理中的三个条件加以合并，得到

定理 8.2.7 G 的非空子集 H 是 G 的子群的充要条件是：对任意的 $a,b\in H$，都有 $ab^{-1}\in H$。

证明：必要性。因为 $a,b\in H$，且 H 是子群，所以 $b^{-1}\in H$，由于 H 对乘法封闭，故 $ab^{-1}\in H$。充分性，只要证明 H 满足群的条件即可，令 $b=a$，则 $aa^{-1}=e\in H$，即 H 中有单位元 e。对于任意的 $h\in H$，有 $eh^{-1}=h^{-1}\in H$，即 H 中任意元素的逆元也在 H 中；最后，对任意

$a,b\in H$，因为 $b^{-1}\in H$，所以 $a(b^{-1})^{-1}\in H$，即 $ab\in H$，故 H 是封闭的，因此 H 是 G 的子群。

这些定理对判断 G 的子集是否为子群有时是十分方便的。

例 8.2.12 设 $G=(Z,+,0)$，$H=\{nk|k\in Z\}$，n 是某个自然数，则 H 是 G 的一个子群。

证明：设 $a,b\in H$，$a=nk_1$，$b=nk_2$，则 $a+b=n(k_1+k_2)\in H$，故 H 是封闭的，又因为 $-a=-nk_1=n(-k_1)\in H$ 且 $(-a)+a=a+(-a)=0\in H$，即 H 中有单位元 0，每个元 a 都有逆元 $-a\in H$，由定理 8.2.6 得证 $H\leqslant G$。

例 8.2.13 设 H_1,H_2 是 G 的两个子群，则 $H=H_1\cap H_2$ 也是 G 的子群。

证明：因为 G 的单位元 $e\in H_1,H_2$，故 $e\in H_1\cap H_2=H$，即 H 是 G 的非空子集，任设 $a,b\in H$，则 $a,b\in H_1$，$a,b\in H_2$，由定理 8.2.7 有 $ab^{-1}\in H_1$，$ab^{-1}\in H_2$，因此 $ab^{-1}\in H$，所以 H 是 G 的子群。

例 8.2.14 设 a 是群 G 中的任一元素，则

$$\langle a\rangle=\{a^k|k\in Z\}\text{ 是 }G\text{ 的子群。}$$

证明：因为 $a^0=e\in\langle a\rangle$，所以 $\langle a\rangle$ 非空。对任意 $a^m,a^n\in\langle a\rangle$，由于

$$a^m(a^n)^{-1}=a^ma^{-n}=a^{m-n}\in\langle a\rangle,$$

由定理 8.2.7，$\langle a\rangle\leqslant G$。

G 的子群 $\langle a\rangle$ 称为由 a 生成的子群，a 称为 $\langle a\rangle$ 的生成元。

例 8.2.15 设 a 是群 G 中的任一元素，令 $c(a)$ 是 G 中与 a 可交换元素的集合，则 $c(a)$ 是 G 的一个子群。

证明：首先 $e\in c(a)$，因为 $ea=ae$；设 $b_1,b_2\in c(a)$，则 $(b_1b_2)a=b_1(b_2a)=b_1(ab_2)=(b_1a)b_2=(ab_1)b_2=a(b_1b_2)$，所以 $b_1b_2\in c(a)$，即 $c(a)$ 是封闭的。另外若 $b\in c(a)$，因为 $ab=ba$，且 b 是 G 中的元素，故 $a=bab^{-1}$，亦即 $b^{-1}a=ab^{-1}$，因此 $b^{-1}\in c(a)$。由定理 8.2.6，$c(a)$ 是 G 的子群。

8.3 循环群 群的同构

给定群 G 的一个非空子集 S，有时需要考虑包含 S 的 G 的最小子群。不妨设 $H(S)$ 和 $H'(S)$ 都是满足条件的子群，那么有 $H(S)\subseteq H'(S)$，同时 $H'(S)\subseteq H(S)$，因此 $H(S)=H'(S)$，即它的存在是唯一的。因为令 $\{H(S)\}$ 是 G 中包含 S 的子群的集合，则所有这些 $H(S)$ 的交集 $\langle S\rangle$ 仍然是 G 的子群，而且它就是包含 S 的 G 的最小子群。称 $\langle S\rangle$ 为由子集 S 生成的子群，S 是群 $\langle S\rangle$ 的生成元集。

如果 S 是一个有限集，不妨设 $S=\{s_1,s_2,\cdots,s_r\}$，我们可以记 $\langle S\rangle=\langle s_1,s_2,\cdots,s_r\rangle$，并且可以构造 $\langle S\rangle$ 如下

$$\langle S\rangle=\{a_1^{\varepsilon_1}a_2^{\varepsilon_2}\cdots a_k^{\varepsilon_k}|a_i\in S,\varepsilon_i\in Z\},$$

即 $\langle S\rangle$ 中包含单位元 e 以及任何元素及它们的逆的乘积。

例 8.3.1 设 $G=(Z_{10},+,\bar{0})$，$S=\{\bar{2},\bar{4}\}$，则 $\langle S\rangle=\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8}\}$；如果 $S=\{\bar{2},\bar{3}\}$，则 $\langle S\rangle=G$；若 $S=\{\bar{1}\}$，则 $\langle S\rangle=G$.

当$\langle S\rangle=G$时，称S是群G的生成元集，即G没有真子群包含S。特别当$\langle S\rangle=G$而且S中只有一个元素a时，有$G=\langle a\rangle$，称G是以a为生成元的循环群。循环群是构造最简单也是最基本的一类群。

定义 8.3.1 若群G中存在一个元素a，使得G中的任意元素g，都可以表示成a的幂的形式，即

$$G=\{a^k \mid k\in Z\},$$

则称G是循环群，记作$\langle a\rangle$，a称为G的生成元。

同样可以定义循环子群。循环子群H是循环群的子群，当然H自身也是一个循环群。

例 8.3.2 $(Z,+,0)$是无限循环群，生成元只有1和-1。

例 8.3.3 $x^n-1=0$在复数域中有n个不同的根

$$x_k=e^{\frac{2k\pi}{n}i},\ k=0,1,\cdots,n-1,$$

称为n次单位根，则

$$U_n=\{e^{\frac{2k\pi}{n}i} \mid k=0,1,\cdots,n-1\}$$

关于乘法运算作成群。令$a=e^{\frac{2\pi}{n}i}$，则$U_n=\langle a\rangle$，即U_n是生成元为a的循环群。

例 8.3.4 设$G=\{a^i \mid i\in Z\}$，$\cdot$是一般乘法运算，则若$O(a)=\infty$、G是无限循环群，a是其生成元；若$O(a)=n$，则$G=\{a^i \mid 0\leqslant i<n\}$，$\langle a\rangle$是有限循环群，由于其周期为$n$所以也称之为$n$阶循环群。

因此，当$G=\langle a\rangle$是循环群时，G的阶与生成元a的阶是一致的，由a的阶的特点可以将循环群分为两类：

1. 当a的阶无限时，$\langle a\rangle$是无限循环群。这时有$O\langle a\rangle=\infty$，

$$\langle a\rangle=\{a^k \mid k\in Z,\ a^m\neq e,m\neq 0\}。$$

2. 当a是有限阶元(n阶)时，$\langle a\rangle$是有限循环群，这时$O\langle a\rangle=n$，

$$\langle a\rangle=\{a^0=e,a,a^2,\cdots,a^{n-1}\}。$$

定理 8.3.1 设$G=\langle a\rangle$，则

1. 若$O\langle a\rangle=\infty$，则G中只有生成元a或a^{-1}。

2. 若$O\langle a\rangle=n$，则G中有$\varphi(n)$个生成元，其中$\varphi(n)$是欧拉函数，它表示小于n且与n互素的正整数个数。

证明：对于$O\langle a\rangle=\infty$，即G是无限循环群时，显见a是生成元，由于$a=(a^{-1})^{-1}$，故对任意$a^k\in G$，$a^k=(a^{-1})^{-k}$，$-k\in Z$，所以a^{-1}也是G的一个生成元。再证无其它生成元：设$G\subset\langle a^m\rangle$，则因为$a\in G$，存在$n$使$(a^m)^n=a$，即$a^{mn-1}=e$，由于$O(a)=\infty$，所以必有$mn-1=0$，故$m=1$或$-1$。

也就是说$\langle a\rangle$中只有两个生成元a和a^{-1}。

下面证明第二部分，若$G=\langle a^r\rangle$，则存在p使$(a^r)^p=a$，即$a^{pr-1}=e$，故则$n\mid(pr-1)$，因而存在$q\in z$使$pr-1=qn$，由此得$(r,n)=1$，而与n互素且小于n的正整数个数为$\varphi(n)$。

例如对于10阶的循环群$\langle a\rangle=\{e,a,a^2,\cdots,a^9\}$，它的全部生成元是$a,a^3,a^7,a^9$。

例 8.3.5 剩余加群$(Z_m,+,\bar{0})$中，所有满足$(k,m)=1$的元素$\bar{k}$都是Z_m的生成元，即$G=\langle\bar{k}\rangle,(k,m)=1$。

在循环群$\langle a\rangle$中任取一个元素a^k，a^k并不一定是生成元，但是由a^k可以生成$\langle a\rangle$的一个子群$\langle a^k\rangle$。那么$\langle a^k\rangle$是不是循环群呢？

定理 8.3.2 设$G=\langle a\rangle$是循环群，则

1.G的子群H都是循环群。

2.若G是无限群，则$H(H\neq\{e\})$也是无限群，若G是有限群时，设$|G|=n$，且a^k是H中a的最小正幂，则$|H|=n/k$。

证明：1.设H是循环群$G=\langle a\rangle$的任一子群，由于a是生成元，因此H中的每个元素都可表示为a的方幂形式，设a^k是H中a的最小正幂，则对任意$a^s\in H$，有$s=pk+r(0\leqslant r<k)$，所以

$$a^r=a^{s-pk}=a^sa^{-pk}=a^s(a^k)^{-p}$$

也是H的元，由于a^k是最小正幂，故$r=0$，即$a^s=(a^k)^p$。所以H中的任意元素都可以表示为a^k的幂的形式，即$H=\langle a^k\rangle$，是循环群。

3.当G是无限循环群时，设$a^k(k\neq0)$是H的一个生成元，且a^k是n阶元，则$(a^k)^n=e$，即$a^{kn}=e$。这与a是无限阶元矛盾，所以a^k是无限阶元，亦即H是无限阶循环群。

当G是有限阶循环群时，设$|G|=n$，所以$O\langle a\rangle=n$，即$a^n=e$，因为H是子群，所以$a^{kn}\in H$，又因为a^k是循环群H中a的最小正幂，所以一定存在一个最小正整数m，使得$(a^k)^m=e=a^n$，即$km=n$。所以a^k的阶$m=\frac{n}{k}$，亦即$|H|=n/k$。

定理 8.3.3 设G是n阶循环群，则对于n的每一个正因子d，G有且只有一个d阶子群。

证明：设$H=\langle a^m\rangle$是G的一个子群，由定理 8.3.2.，$O\langle a^m\rangle=n/m$，即对n的每一个正因子$n/m=d$，G都有d阶子群$\langle a^m\rangle$，以下证其唯一性。因为d是n的任一正因子，令$H=\langle a^{\frac{n}{d}}\rangle$，因为$\left(a^{\frac{n}{d}}\right)^d=a^n=e$，所以$H$是$G$的一个$d$阶子群。设$H_1$是$\langle a\rangle$的任一$d$阶子群，即$H_1=\langle a^k\rangle$，$k$为某一正整数，则由于$(a^k)^d=a^{kd}=e$，所以$kd$是$n$的整倍，设$kd=ln$，于是$k=l\cdot\frac{n}{d}$，由于

$$a^k=a^{l\cdot\frac{n}{d}}=\left(a^{\frac{n}{d}}\right)^l$$

可以表示H为中的生元$a^{\frac{n}{d}}$的幂的形式，所以H_1中的任何元素都是H中的元素，即$H_1\subseteq H$，又由于H_1和H都是d阶子群，所以$H_1=H$。即d阶子群是唯一的。

例如剩余加群$(Z_{14},+)$中14的正因子有1，2，7，和14，因此Z_{14}只有4个子群，即它自身，单位元群$\langle\bar{0}\rangle$，以及$\langle\bar{2}\rangle$和$\langle\bar{7}\rangle$。其中$O\langle\bar{2}\rangle=7$，$O\langle\bar{7}\rangle=2$。

在群中由于指数定律成立，因此循环群一定是交换群，因为$a^ma^n=a^{m+n}=a^{n+m}=a^na^m$。反之，如果有限群$G$是交换群，它必须满足什么条件才是循环群呢？

例 8.3.6 令a，b是阿贝尔群中阶互素的二个元素，$O\langle a\rangle=m$，$O\langle b\rangle=n$，则$\langle a\rangle\cap\langle b\rangle=\{e\}$，且$\langle a,b\rangle=\langle ab\rangle$，$ab$的阶为$mn$。

证明：令$d\in\langle a\rangle\cap\langle b\rangle$，则$d=a^p=b^q$，由于$d^m=(a^p)^m=(a^m)^p=e^p=e$，$d^n=b^{qn}=e$，所

以 $O\langle d\rangle$ 是 m 和 n 因子，但 m 和 n 互素，即 $(m,n)=1$，故 $O\langle d\rangle=1$，所以 $d=e$，因此 $\langle a\rangle\cap\langle b\rangle=\{e\}$。令 $O\langle ab\rangle=r$，则 $(ab)^r=a^rb^r=e$，即在 G 中有 $a^r=b^{-r}$，由于 $a^r\in\langle a\rangle$，$b^{-r}\in\langle b\rangle$，因此 $a^r\in\langle a\rangle\cap\langle b\rangle$，所以 $a^r=e$，$b^r=e$。由于 $O\langle a\rangle=m$，$O\langle b\rangle=n$，所以 $m|r$，$n|r$，亦即 m 和 n 的最小公倍数 $[m,n]$ 可以整除 r，因为 $(m,n)=1$，所以 $[m,n]=mn$，即 $mn|r$。另一方面，$(ab)^{mn}=a^{mn}b^{mn}=(a^m)^n(b^n)^m=e$，所以 $r|mn$。综上，ab 的阶是 mn。以下再证 $\langle a,b\rangle=\langle ab\rangle$，因为 $\langle a,b\rangle$ 是以 $\{a,b\}$ 为生成元的 G 的子群，所以 $\langle a,b\rangle$ 包含 e 以及 ab 的任何乘积形式，即 $\langle a,b\rangle$ 的元素一定是 a^pb^q 形式，其中 $p=1,2,\cdots,m$，$q=1,2,\cdots,n$。所以 $O\langle a,b\rangle\leqslant mn$，。另一方面，由于 ab 是 $\langle a,b\rangle$ 中的一个元素，所以 $\langle ab\rangle\subseteq\langle a,b\rangle$，但因 $O\langle ab\rangle=mn$，故又 $O\langle a,b\rangle\geqslant mn$，因此 $O\langle a,b\rangle=mn$，亦即 $\langle a,b\rangle=\langle ab\rangle$。

例 8.3.7 设 G 是有限阿贝尔群，则 G 中一定有一个元素 g，它的阶是 G 中每个元素阶的整数倍。

证明：设 $a,b\in G$，且 $O\langle a\rangle=m$，$O\langle b\rangle=n$，那么一定会存在一个元素 $c\in G$，满足 $O\langle c\rangle=[m,n]$，为此设 $m=p_1^{i_1}p_2^{i_2}\cdots p_k^{i_k}$，$n=p_1^{j_1}p_2^{j_2}\cdots p_k^{j_k}$，其中 p_i 为不同素数，$i,j\geqslant0$，对 p_i 适当排序后有

$$i_1\leqslant j_1,\cdots,i_t\leqslant j_t,$$
$$i_{t+1}\geqslant j_{t+1},\cdots,i_k\geqslant j_k,\quad(1\leqslant t\leqslant k),$$

并设 $u=p_1^{i_1}\cdots p_t^{i_t}$，$v=p_{t+1}^{j_{t+1}}\cdots p_k^{j_k}$，由于 $m/u=p_{t+1}^{i_{t+1}}\cdots p_k^{i_k}$，$n/v=p_1^{j_1}\cdots p_t^{j_t}$，因此 $[m,n]=m/u\cdot n/v$，其中 $(m/u,n/v)=1$。因为 a 和 b 的阶分别为 m 和 n，所以 G 中一定有二个元素 a^u 和 b^v 的阶分别为 m/u 和 n/v。由例 8.3.6，一定有元素 $c=a^{\frac{m}{u}}b^{\frac{n}{v}}$，它的阶是 $[m,n]$。即为元素 a 和 b 的阶的倍数。同理，如果 G 中还有另一元素 a'，它的阶是 m'，则一定有一个元素，它的阶是 $[[m,n],m']$。如此递归进行，由于 G 是有限群，所以最终一定有一个元素 g，它的阶是 G 中每个元素阶的整数倍。

例 8.3.8 令 G 是有限阿贝尔群，则 G 是循环群的充要条件是 G 的阶为 n，其中 n 是对于 G 中的任何元素 a，满足 $a^n=e$ 的最小正整数。

证明：必要性无需再述。设 G 是满足条件的有限阿贝尔群，如例 8.3.7 的方法选取 G 的元素 g，这样对于 G 中的任何元素 a，都有 $a^{O\langle g\rangle}=e$。因为已知 n 是对任意 a，满足 $a^n=e$ 的最小正整数，所以 $n\leqslant O\langle g\rangle$，但又由于 $|G|=n$，所以 $O\langle g\rangle\leqslant n$，故此 $O\langle g\rangle=n$，即 $G=\langle g\rangle$ 是一个循环群。

下面引入群的同构概念。

定义 8.3.2 设 $(G,\cdot)$ 和 $(G',*)$ 是两个群，$f:G\to G'$ 是双射，如果对任意的 $a,b\in G$，都有

$$f(ab)=f(a)*f(b),$$

则称 f 是 G 到 G' 的一个同构，记作 $G\cong G'$。

例 8.3.9 设 $G=(R^+,\times)$，$G'=(R,+)$，令 $f:x\to\ln x$，则 f 是 G 到 G' 的双射，而且对任意的 $x,y\in G$，

$$f(xy)=\ln(xy)=\ln x+\ln y=f(x)+f(y),$$

因此 $G\cong G'$。

如果把同构的群看成一类，那么循环群只有无限循环群和有限循环群两类。

定理 8.3.4 设 G 是循环群，a 为生成元

1. 若 $O\langle a\rangle=\infty$，则 G 与 $(Z,+)$ 同构。

2. 若 $O\langle a\rangle=n$，则 G 与 $(Z_n,+)$ 同构。

证明：1. 设 $O\langle a\rangle=\infty$，即对任意正整数 $m\neq n$，有 $a^m\neq a^n$，否则若 $a^m=a^n$ 就有 $a^{m-n}=e$，即 $m-n=0,m=n$。

令 $f:a^k\to k$，可以证明 f 是 G 到 Z 的双射。对任意的 $x\in G,x=a^k$，则 $f(x)=f(a^k)=k\in Z$，即 $f(x)$ 由 x 唯一确定，所以 f 是一个映射。任取 $a^m,a^n\in G$，若 $a^m\neq a^n$，则 $m\neq n$，所以 f 是单射。另外任取 $k\in Z$，一定有 $a^k\in G$，使得 $f(a^k)=k$，即 f 是满射，因此 $f:G\to Z$ 是双射。

再设 $x,y\in G,x=a^m,y=a^n$，有

$$f(xy)=f(a^ma^n)=f(a^{m+n})=m+n=f(x)+f(y)。$$

因此 f 是 G 到 Z 的一个同构，$G\cong Z$。

2. 设 a 的周期是 n，则 $a^0=e,a,\cdots,a^{n-1}$ 是 $G=\langle a\rangle$ 中 n 个不同元，同时 G 中也只有 n 个元，因为对任意 $m\in Z$，令 $m=pn+r(0\leqslant r<n)$，有

$$a^m=a^{pn+r}=(a^n)^pa^r=ea^r=a^r。$$

令 $f:a^k\to\bar{k},k=0,1,\cdots,n-1$，与前类似可证 f 是 G 到 Z_n 的双射，并且对任意 $x,y\in G$，设 $x=a^{m_1},y=a^{m_2}(0\leqslant m_1,m_2<n)$，有

$$\begin{aligned}f(xy)&=f(a^{m_1}a^{m_2})=f(a^{m_1+m_2})=(m_1+m_2)\bmod n\\&=f(x)+f(y)。\end{aligned}$$

因此 f 是 G 到 Z_n 的一个同构，即 $G\cong Z_n$。

该定理说明了任两个阶相同的循环群都同构。

例 8.3.10 n 次单位根群 $(U_n,\cdot)$ 与剩余类加群 $(Z_n,+)$ 同构。由例 8.3.3 知 $(U_n,\cdot)$ 是以 $a=e^{\frac{2\pi}{n}i}$ 为生成元的 n 阶循环群，因此 $U_n\cong Z_n$。

关于群的同构，还有一个有用定理。

定理 8.3.5 设 G 是一个群，$(G',\cdot)$ 是一个代数系统，如存在 G 到 G' 的双射 f，且保持运算，即对任意的 $a,b\in G$，有 $f(ab)=f(a)\cdot f(b)$，则 G' 也是一个群。

证明：按照群的定义来验证 G' 是群。

a)证 $\cdot$ 适合结合律，对任何 $a,b,c\in G$，由于 f 是双射，故必唯一存在 $a',b',c'\in G'$，满足 $f(a)=a',f(b)=b',f(c)=c'$，因此

$$\begin{aligned}f((ab)c)&=f(ab)\cdot f(c)=(f(a)\cdot f(b))\cdot f(c)\\&=(a'\cdot b')\cdot c'。\\f(a(bc))&=f(a)\cdot f(bc)=f(a)\cdot(f(b)\cdot f(c))\\&=a'\cdot(b'\cdot c')。\end{aligned}$$

由于 G 中结合律成立，故 $(a'\cdot b')\cdot c'=a'\cdot(b'\cdot c')$，即 G' 是半群。

b)设 e 是 G 的单位元，$f(e)=e'$，可证 e' 是 G' 的单位元。对任意 $a'\in G'$，都存在唯一 $a\in G$，使 $f(a)=a'$，由 $ae=ea=a$ 得 $f(ae)=f(a)\cdot f(e)=a'\cdot e'=a'$，$f(ea)=f(e)\cdot f(a)=e'\cdot a'=a'$，因此 e' 是 G 的单位元。

c)任取 $a'\in G'$，令 $f(a)=a'$，则有 $f(a^{-1})=x\in G'$，所以 $f(aa^{-1})=f(a)\cdot f(a^{-1})=a'\cdot x=e'$，$f(a^{-1}a)=f(a^{-1})\cdot f(a)=x\cdot a'=e'$，所以 a' 在 G' 中有逆元 x，因此 $(G',\cdot)$ 是群。

8.4 变换群和置换群 Cayley 定理

设 $A=\{a_1,a_2\cdots\}$ 是一个非空集合，A 到 A 的一个映射 f 称为 A 的一个变换，记作

$$f:\begin{bmatrix} a_1 & a_2 & \cdots \\ f(a_1) & f(a_2) & \cdots \end{bmatrix}$$

对于 A 中的两个变换 f,g，可以得到 A 得另一个变换 gf。

$$gf(a)=g(f(a)),\ 对任意\ a\in A。$$

gf 称为变换 f 与 g 的乘积。容易验证，变换乘法适合结合律。设 f 是 A 中任一变换，都满足

$$fI=If=f。$$

其中 I 是 A 中的恒等变换。

这样，A 上的全部变换的集合 $M(A)$ 对于变换的乘法运算构成幺群。设 $|A|=n$，则 A 到自身的不同映射一共有 n^n 个。如果变换 f 是双射，称其为一一变换。对于 A 上任一个一一变换 f，也一定存在一个一一变换 f^{-1}，满足 $ff^{-1}=f^{-1}f=I$，称 f^{-1} 是 f 的逆变换。这样幺群 $(M(A),\cdot)$ 中的全部一一变换构成的集合 $E(A)$，对于变换的乘法运算构成群，称它为 A 的一一变换群。

定义 8.4.1 非空集合 A 的所有一一变换关于变换的乘法所作成的群叫做 A 的一一变换群，用 $E(A)$ 表示，$E(A)$ 的子群叫做变换群。

例 8.4.1 设 A 是平面上所有点构成的集合，则平面上绕某定点的一个旋转是 A 的一个一一变换。设 G 是所有绕该定点旋转的集合，则

1. $\varphi_{\theta_1}\cdot\varphi_{\theta_2}=\varphi_{\theta_1+\theta_2}$

仍然是一个旋转，所以 G 对与运算 $\cdot$ 是封闭的。

2. $\varphi_{\theta_1}\cdot(\varphi_{\theta_2}\cdot\varphi_{\theta_3})=\varphi_{\theta_1+\theta_2+\theta_3}=(\varphi_{\theta_1}\cdot\varphi_{\theta_2})\cdot\varphi_{\theta_3}$。

3. $e=\varphi_{\theta=0}$。

4. 对任意 $\varphi_\theta\in G$，都有逆旋转 $\varphi_{-\theta}\in G$，满足

$$\varphi_\theta\cdot\varphi_{-\theta}=\varphi_{-\theta}\cdot\varphi_\theta=\varphi_0=e。$$

所以 $(G,\cdot)$ 是一个变换群。

当 A 是一个有限集合时，例如 $A=\{1,2,\cdots,n\}$，A 中的一个一一变换称为一个 n 元置换，由置换构成的群叫置换群。因此置换群是变换群的一个特殊类型。为了便于讨论置换群，我们首先回顾一下置换与置换乘法。

对于 A 中的一个 n 元置换 $\sigma:i\to\sigma(i)$，$i=1,2,\cdots,n$，我们记作

$$\sigma=\begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}$$

例如对 3 元置换 $\sigma:1\to3,2\to1,3\to2$，可表示为

$$\sigma=\begin{bmatrix}1 & 2 & 3\\3 & 1 & 2\end{bmatrix}$$

由于置换是一一变换(双射),所以$\sigma(1),\sigma(2),\cdots,\sigma(n)$是1到$n$的一个排列,反之对1到$n$的任一个排列$\sigma(1),\sigma(2),\cdots,\sigma(n)$,都唯一地对应有一个$n$元置换,因此$A$中一共有$n!$个$n$元置换(注意变换幺群$M(A)$中有$n^n$个变换),我们用$S_n$表示这$n!$个$n$元置换的集合。

例 8.4.2 设$A=\{1,2,3\}$,则$S_3=\{\sigma_1,\sigma_2,\cdots,\sigma_6\}$,其中

$$\sigma_1=\begin{bmatrix}1 & 2 & 3\\1 & 2 & 3\end{bmatrix}\quad \sigma_2=\begin{bmatrix}1 & 2 & 3\\1 & 3 & 2\end{bmatrix}\quad \sigma_3=\begin{bmatrix}1 & 2 & 3\\2 & 1 & 3\end{bmatrix}$$

$$\sigma_4=\begin{bmatrix}1 & 2 & 3\\2 & 3 & 1\end{bmatrix}\quad \sigma_5=\begin{bmatrix}1 & 2 & 3\\3 & 1 & 2\end{bmatrix}\quad \sigma_6=\begin{bmatrix}1 & 2 & 3\\3 & 2 & 1\end{bmatrix}$$

在该例中可以计算置换的乘法,比如$\sigma_2\sigma_4$,因为$\sigma_2\sigma_4:i\to\sigma_2(\sigma_4(i))$,所以$\sigma_2(\sigma_4(1))=\sigma_2(2)=3,\sigma_2(\sigma_4(2))=\sigma_3(3)=2,\sigma_2(\sigma_4(3))=\sigma_2(1)=1$,因此

$$\sigma_2\sigma_4=\begin{bmatrix}1 & 2 & 3\\1 & 3 & 2\end{bmatrix}\begin{bmatrix}1 & 2 & 3\\2 & 3 & 1\end{bmatrix}=\begin{bmatrix}1 & 2 & 3\\3 & 2 & 1\end{bmatrix}=\sigma_6。$$

对于S_n中的任意两个置换σ,τ,它们的乘积

$$\sigma\tau=\begin{bmatrix}1 & 2 & \cdots & n\\\sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{bmatrix}\begin{bmatrix}1 & 2 & \cdots & n\\\tau(1) & \tau(2) & \cdots & \tau(n)\end{bmatrix}$$

其中$\sigma\in S_n$也可以表示为

$$\sigma=\begin{bmatrix}k_1 & k_2 & \cdots & k_n\\\sigma(k_1) & \sigma(k_2) & \cdots & \sigma(k_n)\end{bmatrix}$$

其中$k_1,k_2,\cdots,k_n$是1到n的一个排列,所以

$$\begin{aligned}\sigma\tau&=\begin{bmatrix}\tau(1) & \tau(2) & \cdots & \tau(n)\\\sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n))\end{bmatrix}\begin{bmatrix}1 & 2 & \cdots & n\\\tau(1) & \tau(2) & \cdots & \tau(n)\end{bmatrix}\\&=\begin{bmatrix}1 & 2 & \cdots & n\\\sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n))\end{bmatrix}\end{aligned}$$

仍然是S_n中的置换。

在S_n中,恒等置换是

$$e=\begin{bmatrix}1 & 2 & \cdots & n\\1 & 2 & \cdots & n\end{bmatrix}$$

对于任意$\sigma\in S_n$,都有$\sigma e=e\sigma=\sigma$,同时由于

$$\begin{bmatrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\1 & 2 & \cdots & n\end{bmatrix}\begin{bmatrix}1 & 2 & \cdots & n\\\sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{bmatrix}=e,$$

$$\begin{bmatrix}1 & 2 & \cdots & n\\\sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{bmatrix}\begin{bmatrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\1 & 2 & \cdots & n\end{bmatrix}=e,$$

所以σ有逆置换。

$$\sigma^{-1}=\begin{bmatrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\1 & 2 & \cdots & n\end{bmatrix}$$

由上可以得到如下定义：

定义 8.4.2 S_n 对于置换乘法构成群，称为 n 次对称群。S_n 的子群称为 n 元置换群。

为了便于研究置换群，可以将置换的表示加以简化。首先分析置换的性质。

设置换 σ 满足 $\sigma(i_1)=i_2, \sigma(i_2)=i_3, \cdots, \sigma(i_l)=i_1$，其中 $\sigma(i_j)=i_{j+1}, 1\leqslant j<l$，则称 $(i_1, i_2, \cdots, i_l)$ 是一个长度为 l 的轮换。当 $l=1$ 时称为恒等置换，当 $l=2$ 时称之为对换。一般情况下我们可以记 $\gamma=(i_1\, i_2 \cdots\, i_l)$，当然也可以把 γ 表示为

$$\gamma=(i_2\, i_3 \cdots\, i_l\, i_1)=(i_3\, i_4 \cdots\, i_l\, i_1\, i_2) \text{ 等等。}$$

这时 γ^2 也是一个映射：$\gamma^2(i_1)=i_3, \gamma^2(i_2)=i_4, \cdots$，一般设 $1\leqslant k\leqslant l$ 时，有

$$\gamma^k(i_j)=i_{j+k},\ j+k\leqslant l。$$

$$\gamma^k(i_j)=i_{j+k-l},\ j+k>l。$$

显然，$\gamma^l=e$，而 $\gamma^k\neq e(1\leqslant k<l)$，所以 γ 的阶是 l。例如设置换

$$\gamma=\begin{bmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 2 & 1\end{bmatrix}$$

可以把它写成轮换的形式：$\gamma=(1\ 3\ 2\ 4)$，并且此时 $\gamma^4=e$。

定义 8.4.3 设 α, β 是 S_n 中的两个轮换，如果 α 和 β 中的元素都不相同，则称 α 和 β 是不相交的。

例如设 $\alpha=(1\ 3\ 6), \beta=(2\ 5)$，它们是不相交的。因此如果设 $\alpha(i)\neq i$，那么 $\alpha\beta(i)=\alpha(i), \beta\alpha(i)=\alpha(i)$，类似地，如果设 $\beta(i)\neq i$，那么 $\alpha\beta(i)=\beta(i)=\beta\alpha(i)$，因此对任意 i，都有 $\alpha\beta(i)=\beta\alpha(i)$，故 $\alpha\beta=\beta\alpha$。

定理 8.4.1 设 α、β 是两个不相交的轮换，则 $\alpha\beta=\beta\alpha$。

也就是说，不相交轮换的乘法满足交换律。

设 α 是若干个不相交轮换的乘积，比如

$$\alpha=(i_1\, i_2 \cdots\, i_p)(j_1\, j_2 \cdots\, j_q)\cdots(k_1\, k_2 \cdots\, k_r)。$$

令 $p, q, \cdots, r$ 的最小公倍数是 m，那么 m 就是置换 α 的阶。因为设 $\alpha_1=(i_1\, i_2 \cdots\, i_p), \alpha_2=(j_1\, j_2 \cdots\, j_q), \cdots, \alpha_t=(k_1\, k_2 \cdots\, k_r)$，那么 $\alpha=\alpha_1\alpha_2\cdots\alpha_t$，而 $\alpha^m=\alpha_1^m\alpha_2^m\cdots\alpha_t^m$，由于 $\alpha_i^m=e$，因此 $\alpha^m=e$。反之，设 $\alpha^n=e$，由于 α_i, α_j 是不相交轮换，所以一定有 $\alpha_i^n=e$，因此 n 是 $p, q, \cdots, r$ 的整数倍。当然 n 也一定是它们的最小公倍数 m 的整数倍。因此 α 的阶是 m。

如果 σ 是 S_n 中的一个 n 元置换，那么它一定能表示成轮换的乘积。

例 8.4.3 设 n 元置换

$$\sigma=\begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 3 & 5 & 1 & 4 & 6 & 7 & 2\end{bmatrix}$$

则 $\sigma(1)=3, \sigma(3)=1, \sigma(2)=5, \sigma(5)=6, \sigma(6)=7, \sigma(7)=2, \sigma(4)=4$，所以 $\sigma=(1\ 3)(2\ 5\ 6\ 7)(4)$。其中 (4) 是长度为 1 的轮换，亦即恒等置换。它可以省略，故此 $\sigma=(1\ 3)(2\ 5\ 6\ 7)$。

定理 8.4.2 任何置换都可表为不相交轮换的乘积。

例 8.4.4 S_4 的全部置换可表为

1. $e=(i)$。

2. $(1\ 2), (3\ 4), (1\ 3), (2\ 4), (1\ 4), (2\ 3)$。

3. $(1\ 2\ 3), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 3), (1\ 2\ 4), (1\ 4\ 2), (2\ 3\ 4), (2\ 4\ 3)$。

4. (1 2 3 4), (1 2 4 3), (1 3 2 4), (1 3 4 2), (1 4 2 3), (1 4 3 2)。

5. (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)。

因为轮换实质上也是置换，所以轮换的乘法运算直接用置换乘法进行。

例 8.4.5 设 $f_1=(1\ 3\ 4)(2\ 5)$，$f_2=(1\ 5\ 3)(2\ 4)$，则

$$\begin{aligned} f_1 f_2 &= (1\ 3\ 4)(2\ 5)(1\ 5\ 3)(2\ 4) \\ &= (1\ 2)(3)(4\ 5) \\ &= (1\ 2)(4\ 5)。\end{aligned}$$

同时，任何一个轮换 σ 都可以表为对换的乘积。例如

$$(i_1\ i_2 \cdots i_l) = (i_2\ i_3)(i_3\ i_4)\cdots(i_{l-1}\ i_l)(i_1\ i_l),$$

或者

$$(i_1\ i_2 \cdots i_l) = (i_1\ i_l)(i_1\ i_{l-1})\cdots(i_1\ i_3)(i_1\ i_2)。$$

虽然它们的表示形式不一样，但是它们所含对换的个数都是一样的，即含 $(l-1)$ 个对换。因此设置换 $\sigma=\sigma_1\sigma_2\cdots\sigma_k$，其中 σ_i 是一长度为 l_i 的轮换，且 σ_i 与 σ_j 是不相交的轮换，那么 σ 用上述方法表成对换乘积的形式后，它所含的对换数为

$$N(\sigma) = \sum_{j=1}^{k}(l_i - 1)。$$

可以证明，不管用什么方法把置换表成对换之积，所得对换的个数与 $N(\sigma)$ 的奇偶性相同。如果 $N(\sigma)$ 是奇数，称 σ 是奇置换，否则称为偶置换。

由奇、偶置换的定义可知，奇置换乘奇置换得偶置换，偶置换乘偶置换也是偶置换，奇、偶置换间相乘是奇置换，即

$$N(\sigma_1\sigma_1) = N(\sigma_1) + N(\sigma_2)\ (\text{mod } 2)。$$

例 8.4.6 在例 8.4.4 中

(1 3 2)(1 3)(2 4)=(1 2 4)，偶置换的乘积为偶置换。(1 2 4 3)(1 3 2 4)=(2 3 4)，奇置换的乘积为偶置换，(1 3 2)(1 2 4 3)=(2 4)，奇偶置换间相乘为奇置换。

由此可以得出

定理 8.4.3 n 次对称群 S_n 中所有偶置换的集合，对于 S_n 中的置换乘法构成子群，记为 A_n，称为交错群，若 $n\geqslant 2$，则 $|A_n|=\frac{1}{2}n!$。

比如例 8.4.4 的 S_4 中，1，3，5 类是偶置换，它们构成交错群 A_4，且 $|A_4|=12$。

证明：因为 S_n 是有限群，而且任意两个偶置换的乘积仍然是偶置换，由定理 8.2.7 可知，S_n 中所有偶置换构成 S_n 的一个子群。假定 S_n 中偶置换数为 n_1，奇置换数为 n_2。由某个奇置换去乘所有不同的偶置换，就会得到群 S_n 中互异的奇置换，故 $n_1\leqslant n_2$。同理 $n_2\leqslant n_1$，因此 $|A_n|=\frac{1}{2}|S_n|=\frac{1}{2}n!$。

变换群在群论中占有特殊的地位，因为就同构的意义上来讲，任何一个抽象幺群都和一个变换幺群同构。同样，任何一个抽象群都与一个变换群同构。

定理 8.4.4 (Cayley 定理) 任意群 G 与一个变换群同构。

证明：首先需要构造一个变换群，任取 $a\in G$，定义 G 上的一个变换 $f_a: x\to ax$，对任意的 $x\in G$。以下要证明 f_a 是一一变换，而且 $\{f_a\,|\,a\in G\}$ 对变换乘法构成群。

由于群 G 中方程 $ax=b$ 有唯一解，所以对任意的 $b\in G$，都存在有元素 $x\in G$，使 f_a

$(x)=b$，因此 f_a 是满射。同时对 $x_1,x_2\in G$，$x_1\neq x_2$ 时，有 $ax_1\neq ax_2$，即 $f_a(x_1)\neq f_a(x_2)$，因此 f_a 又是单射，故 f_a 是一一变换。

其次证 $\overline{G}=\{f_a|a\in G\}$关于变换乘法成群。对任意的 $f_a,f_b\in\overline{G}$，

$$(f_a f_b)(x)=f_a(f_b(x))=f_a(bx)=abx=f_{ab}(x)。$$

由于 $a,b\in G$，所以 $ab\in G$，即 $f_{ab}\in\overline{G}$，因此 $\overline{G}$ 对于变换乘法运算是封闭的。同时它存在单位元 $f_e:x\to ex$，而且对任意 $a\in G$，因为 $f_a^{-1}f_a=f_af_a^{-1}=e$，所以 f_a 都有其逆元 $f_a^{-1}=f_a^{-1}$。因此$(\overline{G},\cdot)$是变换群。

以下证明 G 和变换群 $\overline{G}$ 同构。

令 $\varphi:a\to f_a$。对任意 $a,b,x\in G$，若 $a\neq b$，则 $ax\neq bx$，因此 $f_a\neq f_b$，亦即 $\varphi(a)\neq\varphi(b)$，故 φ是 G 到 $\overline{G}$ 的单射。同时，对任意的 $f_a\in\overline{G}$，都存在 $a\in G$，使 $\varphi(a)=f_a$，因此 φ 是满射，所以 φ 是 G 到 $\overline{G}$ 的双射。又由于

$$\varphi(ab)=f_{ab}=f_a f_b=\varphi(a)\varphi(b),$$

即 φ 保持运算，故 $G\cong\overline{G}$。

推论：设 G 是 n 阶有限群，则 G 与 S_n 的一个子群同构。

例 8.4.7 设 $G=\langle a\rangle$是 n 阶循环群，则 G 与 S_n 的一个子群 $\overline{G}$ 同构。由于 G 是循环群，所以 $\overline{G}$ 也是循环群，因此只要找到 $\overline{G}$ 的生成元就可以确定 $\overline{G}$。由于 $G\cong\overline{G}$，所以 G 中生成元 a 的象就是 $\overline{G}$ 中的生成元。设 a 的象是 $f_a:x\to ax$，有

$$f_a=\begin{bmatrix} e & a & a^2 & \cdots & a^{n-1} \\ a & a^2 & a^3 & \cdots & e \end{bmatrix}=[e \quad a \quad a^2 \quad \cdots \quad a^{n-1}],$$

因此

$$\overline{G}=\langle(e\ a\ a^2\cdots a^{n-1})\rangle。$$

8.5 陪集和群的陪集分解 Lagrange 定理

设 G 是一个群，H 是 G 的子群，利用 H 可以在 G 的元素之间确定一个二元关系 R：

$$a\ R\ b \quad \text{当且仅当 } ab^{-1}\in H。$$

这样对任意 $a,b\in G$，可以确定 ab^{-1}是否属于 H，因此 R 是 G 中的一个二元关系，而且也是等价关系，因为

1. $aa^{-1}=e\in H$，所以 $a\ R\ a$。
2. 由 $ab^{-1}\in H$，可知$(ab^{-1})^{-1}\in H$，即 $ba^{-1}\in H$，也就是说，若 $a\ R\ b$，则 $b\ R\ a$。
3. 若 $ab^{-1}\in H$，$bc^{-1}\in H$，则

$$(ab^{-1})(bc^{-1})=a(b^{-1}b)c^{-1}=ac^{-1}\in H,$$

即 $a\ R\ b\wedge b\ R\ c\to a\ R\ c$。

因此由等价关系 R 可以唯一确定 G 的一个划分，其划分的块就是子群 H 的陪集。

定义 8.5.1 设 H 是群 G 的一个子群，对任意的 $a\in G$，集合

$$aH=\{ah|h\in H\}。$$

称为子群 H 在 G 中的一个左陪集。同理，H 在 G 中的一个右陪集是

$$Ha=\{ha|h\in H\}。$$

例 8.5.1 设 $G=S_3, H=\{e,(1\ 2)\}$，对 a 取 $e,(1\ 3)$和$(2\ 3)$时，其左陪集分别是

$$eH=H=\{e,(1\ 2)\}。$$
$$(1\ 3)H=\{(1\ 3),(1\ 2\ 3)\}。$$
$$(2\ 3)H=\{(2\ 3),(1\ 3\ 2)\}。$$

而对应的右陪集是

$$He=H。$$
$$H(1\ 3)=\{(1\ 3),(1\ 3\ 2)\}。$$
$$H(2\ 3)=\{(2\ 3),(1\ 2\ 3)\}。$$

因此一般情况下 $Ha\neq aH$。

例 8.5.2 设 $G=S_3, H=\{e,(1\ 2\ 3),(1\ 3\ 2)\}$是交错群 A_3，对 a 分别取$(1\ 2\ 3)$和$(1\ 2)$时，可以得到 H 的左陪集。

$$(1\ 2\ 3)H=\{(1\ 2\ 3),(1\ 2\ 3)^2,(1\ 2\ 3)(1\ 3\ 2)\}$$
$$=\{(1\ 2\ 3),(1\ 3\ 2),e\}=H。$$
$$(1\ 2)H=\{(1\ 2),(1\ 2)(1\ 2\ 3),(1\ 2)(1\ 3\ 2)\}$$
$$=\{(1\ 2),(2\ 3),(1\ 3)\}。$$

同理可得右陪集。

$$H(1\ 2\ 3)=\{(1\ 2\ 3),(1\ 3\ 2),e\}=H。$$
$$H(1\ 2)=\{(1\ 2),(2\ 3),(1\ 3)\}。$$

事实上，对任意的对称群 S_n，当 $H=A_n$ 时总有 $aH=Ha$，其中 $a\in S_n$。

下面我们以左陪集为例介绍陪集的性质。

定理 8.5.1 设 H 是 G 的子群，则 H 的左陪集具有下述性质

1. $H=eH, a\in aH$。
2. $|aH|=|H|$。
3. $a\in H <=> aH=H$。
4. 对任意的 $x\in aH$，都有 $xH=aH$，并称 a 是 aH 的一个陪集代表。
5. $aH=bH <=> a\in bH$ 或 $b\in aH <=> a^{-1}b\in H$ 或 $b^{-1}a\in H$。
6. 对任意的 $a,b\in G$，若非 $aH=bH$，则 $aH\cap bH=\phi$。

证明：

1. 因为 $e\in H$，所以 $eH=\{eh|h\in H\}=\{h|h\in H\}=H$，同时 $a=ae\in\{ah|h\in H\}=aH$。

2. 因为 $H\leqslant G$，对任意 $h_1,h_2\in H$，若 $h_1\neq h_2$，则 $ah_1\neq ah_2, a\in G$，所以 aH 中没有共同元素且 $|aH|=|H|$。

3. 因为 $a\in H$，所以 $aH=\{ah|h\in H\}=\{h'|h'\in H\}\subseteq H$，又由于 $|aH|=|H|$，故 $aH=H$。

4. 对任意的 $x\in aH$，设 $x=ah_1, h_1\in H$，则对任意 $xh\in xH$，有 $xh=(ah_1)h=a(h_1h)=ah'$，其中 $h'\in H$。因此 $ah'\in aH$，亦即 $xH\subseteq aH$。反之，若 $x=ah_1$，就有 $a=xh_1^{-1}$，其中 $h_1^{-1}\in H$，故此对任意 $ah\in aH$，都有 $ah=(xh_1^{-1})h=x(h_1^{-1}h)\in xH$，亦即 $aH\subseteq xH$，因此性质 4 得证。

5. 先证必要性，因为 $aH=bH$，由性质 1，$a\in aH=bH$，故 $a\in bH$，由此存在元素 $h\in H$，满足 $a=bh$，因而 $b^{-1}a=h\in H$；再证充分性，因为 $a^{-1}b\in H$，所以存在 $h_1\in H$，满足$a^{-1}b=h_1$，因而在群 G 中有 $b=ah_1$，亦即 $b\in aH$；又由性质 4，$bH=aH$，至于性质的另一半，由于 a 与 b 是对称存在的，所以不证自明。

6. 若 $aH\cap bH\neq\phi$，则存在一个元素 x，$x\in aH\cap bH$，这时 $x\in aH$，$x\in bH$。由性质 4，$xH=aH=bH$，故得证。

由性质 6 可以得到

定理 8.5.2 设 G 是有限群，H 是 G 的子群，则存在一个正整数 k，满足

$$G = a_1H \cup a_2H \cup \cdots \cup a_kH,$$

其中 $a_iH\cap a_jH=\varnothing$，$i\neq j$，$i,j=1,2,\cdots,k$

比如例 8.5.1 中，$G=H\cup(1\ 3)H\cup(2\ 3)H$，例 8.5.2 中，$G=H\cup(1\ 2)H$。如果 G 是无限群，它的陪集分解可能是无限的，也可能是有限的。

例 8.5.3 设 $G=(R^*,\cdot)$，$H=\{1,-1\}$是 G 的子群，于是

$$G = \bigcup_{a\in R^+} aH$$

其中 R^+是正实数集，R^*是非零实数集，因此 G 分解为无限个陪集。

例 8.5.4 设 $G=\langle a\rangle$是无限循环群，$H=\{\cdots,a^{-2},e,a^2,\cdots\}$是 G 的子群，则 $G=H\cup aH$，它只分解为二个陪集。

群的右陪集分解的性质与左陪集完全类似，虽然在许多情况下 H 的左、右陪集不一定相等。($aH\neq Ha$)，但是它的左右陪集的个数是相等的，即它们或者就是无限大或者都是有限而且数目相等。下面的定理给出了这个结论。

定理 8.5.3 H 是 G 的一个子群，设 H 的左右陪集的集合分别是 S_L、R_L。

$$S_L = \{aH|a \in G\}\ ,\ R_L = \{Ha|a \in G\}。$$

则存在 S_L 到 R_L 的一个双射 σ。

证明：令 $\sigma:aH\to Ha^{-1}$，我们将证明 σ 是双射。首先证明相同的左陪集在 R_L 中的象也相同，亦即 $aH=bH \Leftrightarrow Ha^{-1}=Hb^{-1}$。因为 $aH=bH \Leftrightarrow a^{-1}b\in H \Leftrightarrow (a^{-1})(b^{-1})^{-1}\in H$，且由于定理 8.5.1 的性质 4 对右陪集而言可表为 $Ha=Hb \Leftrightarrow ab^{-1}\in H$，因此$(a^{-1})(b^{-1})^{-1}\in H \Leftrightarrow Ha^{-1}=Hb^{-1}$。该结论一方面说明一个左陪集在 R_L 中的象与该陪集的代表元选择无关，另一方面也说明若 $aH\neq bH$，则 $Ha^{-1}\neq Hb^{-1}$，即 $\sigma(aH)\neq\sigma(bH)$，故 σ 是单射。反之，对任意的 $Ha\in R_L$，都有 $\sigma(a^{-1}H)=H(a^{-1})^{-1}=Ha$，即存在原象 $a^{-1}H\in S_L$，因此 σ 是满射，故 σ 是双射，即 S_L 与 R_L 之间存在一一对应关系。这样我们得到如下定义

定义 8.5.2 群 G 关于其子群 H 的左(右)陪集的个数，称为 H 在 G 中的指数，记作$[G:H]$。

例 8.5.5 若 $H=\{e\}$，则 $S_L=\{\{a\}|a\in G\}$，因此$[G:\{e\}]=|G|$，或记作$[G:1]$。

在例 8.5.1 中，$[G:H]=3$，而且每一个左陪集都与 H 含有相同数目的元素。在有限群 G 中，由于每一个左陪集 aH，都有 $|aH|=|H|$，而且 G 中共有$[G:H]$个不同的左陪集，加之这些左陪集构成了 G 的一个分解，因此$|G|=[G:H]\cdot|H|$，于是我们得到了

·个重要定理。

Lagrange 定理. 设 G 是有限群，H 是 G 的子群，则 $[G:1]=[G:H][H:1]$。

该定理说明一个有限群 G 的子群 H 的阶只可能是 G 的阶的因子，比如 G 是 10 阶的群，那么它最多只有 1 阶、2 阶、5 阶和 10 阶的子群，而不可能有 3 阶、4 阶等等子群。从 Lagrange 定理可以得到以下几个重要推论。

推论 1. 设有限群 G 的阶为 n，则 G 中任意元素的阶都是 n 的因子，且适合 $x^n=e$。

证明：设 a 是 G 中的任一元素，由 a 生成的 G 的一个循环子群 $H=\langle a\rangle$，由 Lagrange 定理知 H 的阶是 n 的因子，而 $|H|=O\langle a\rangle$，因此 $O\langle a\rangle \mid [G:1]$，设 $O\langle a\rangle=m$，则一定存在正整数 k，满足 $n=km$，所以 $a^n=a^{km}=(a^m)^k=e^k=e$，即 G 中任意元素 a 都适合方程 $x^n=e$。

推论 2. 阶为素数 p 的群 G 是循环群。

证明：任取 G 中一非单位元 a，由 a 生成的循环群 $\langle a\rangle$ 是 G 的子群，且 $\langle a\rangle$ 不是单位元群，即 $O\langle a\rangle>1$，由于 p 是素数，故 $p>1$，又由于 $O\langle a\rangle \mid p$，所以 $O\langle a\rangle=p$，即 $G=\langle a\rangle$。

推论 3. 设 A、B 是群 G 的两个有限子群，则

$$|AB| = \frac{|A||B|}{|A\cap B|}$$

其中 $AB=\{ab \mid a\in A, b\in B\}=\bigcup\limits_{a\in A} aB$。

证明：因为 B 是 G 的子群，所以 aB 是 B 的一个左陪集。设 $S_1=\{aB \mid a\in A\}=\{a_1B, a_2B, \cdots, a_mB\}$，再令 $D=A\cap B$，可知 D 是 G 的子群，同时也是 A 的子群，因此 $A=\bigcup aD$，设 $S_2=\{aD \mid a\in A\}=\{a_1D, a_2D, \cdots, a_nD\}$。我们在 S_1 和 S_2 之间建立一种关系，$\sigma: a_iB\to a_iD$。由于陪集的性质，对任意 $a_i, a_j\in A$，若 $a_iB=a_jB$，则有 $a_i^{-1}a_j\in B$；同时因为 $a_i, a_j\in A$ 且 A 是群，故 $a_i^{-1}a_j\in A$，因此 $a_i^{-1}a_j\in A\cap B$，即 $a_i^{-1}a_j\in D$，它等价于 $a_iD=a_jD$。所以 σ 是映射且是单射。同时对于任意的 $a_iD\in S_2$，都存在 $a_i\in A$，亦即有 $a_iB\in S_1$，满足 $\sigma(a_iB)=a_iD$，故 σ 是满射，因此 σ 是双射，亦即 $|S_1|=|S_2|=k$。因此

$$|AB| = |\bigcup_{a\in A} aB| = k|B|, \quad |A| = k|D|。$$

用 $k=|A|/|D|$ 代入前式就有

$$|AB| = \frac{|A||B|}{|A\cap B|}$$

例 8.5.6 设 G 是阶为 4 的群，则 G 或是循环群，或是 Klein 四元群。

证明：若有 $a\in G$，且 a 的周期是 4，则 $\langle a\rangle$ 是 G 的循环子群，且 $\langle a\rangle=G$，所以 G 就是循环群。否则 G 中不含周期为 4 的元，这样除单位元外，由 Lagrange 定理，其余元素的周期只能都是 2。设 $G=\{e,a,b,c\}$，应有 $a^2=b^2=c^2=e$。又因为 $a,b\in G$，且消去律成立，所以 $ab\neq a$，$ab\neq b$，且 $ab\neq e$，故此 $ab=c$。同理 $ac=b$，$bc=a$，…，因此 G 的乘法表如下：

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

它就是 Klein 四元群。

例 8.5.7 设 a,b 是群 G 中的二个元素，$O\langle a\rangle=m$，$O\langle b\rangle=n$，且 m 和 n 互素，又设在 G 中 $ab=ba$，证明 $O\langle ab\rangle=mn$。

证明：设 ab 的周期为 k，因为 $(ab)^{mn}=a^{mn}b^{mn}=e$，因此 $k\mid mn$，由于 $(ab)^k=a^kb^k=e$，所以 $a^k=b^{-k}\in\langle b\rangle$，即 $\langle a^k\rangle$ 是 $\langle b\rangle$ 的子群。由 Lagrange 定理知 $\langle a^k\rangle$ 的阶是 $\langle b\rangle$ 的阶的因子。同时因为 $a^k\in\langle a\rangle$，因此 $\langle a^k\rangle$ 也是 $\langle a\rangle$ 的子群，同样 $O\langle a^k\rangle\mid O\langle a\rangle$，也就是说 $\langle a^k\rangle$ 的阶是 m 和 n 的公因子，由于 $(m,n)=1$，所以 $O\langle a^k\rangle=1$，即 $a^k=e$，同时 $b^k=e$，亦即 $m\mid k,n\mid k$，因此 k 是 m,n 的倍数，而且满足 $k=[m,n]$，因此 $k=mn$。

8.6 正规子群与商群

从上节中我们看到，在许多情况下群 G 的子群的左右陪集并不相等，但是有些子群 H，能够对 G 中的任意元 a，满足 $aH=Ha$，比如例 8.5.2 就属于这种情况，这样的子群叫做正规子群。

定义 8.6.1 设 H 是 G 的一个子群，如果对任意的 $a\in G$，都有 $aH=Ha$，则称 H 是 G 的一个正规子群(亦称不变子群)，用符号 $H<G$ 表示。

因此，对正规子群 H 就不必区分其左右陪集，而简称为 H 的陪集。

例 8.6.1 阿贝尔群的任一个子群都是正规子群。因为设 $H=\{h_1,h_2,\cdots,h_m\}$，对任意的 $a\in G$，有

$$aH=\{ah_1,ah_2,\cdots,ah_m\}=\{h_1a,h_2a,\cdots,h_ma\}=Ha。$$

例 8.6.2 G 的平凡子群 $\{e\}$ 和 G 都是 G 的正规子群。

例 8.6.3 A_n 是 S_n 的正规子群。因为 A_n 是 S_n 中全部偶置换的集合，由于偶置换之积是偶置换，奇置换与偶置换之积是奇置换，所以对 S_n 中的任一置换 σ，都有 $\sigma A_n=A_n\sigma$，故 A_n 是 S_n 的正规子群。

例 8.6.4 设 H 是 G 的一个子群，且 $[G:H]=2$，则 H 是 G 的正规子群。

证明：任取 G 中的一个元素 a，若 $a\in H$，则 $aH=H=Ha$，若 $a\notin H$，则 $aH\neq H$，由于 $[G:H]=2$，所以 $G=aH\cup H$，同样，H 的右陪集 $Ha\neq H$，亦有 $G=Ha\cup H$，因此 $aH\cup H=Ha\cup H$，比较两端得到 $aH=Ha$，结论正确。

给定 G 的一个子群 H，怎样判断 H 是否为 G 的正规子群呢？

定理 8.6.1 设 H 是 G 的子群，则以下几个条件等价：

1. $H\lhd G$。

2. 对任意 $g\in G$，$gHg^{-1}=H$。

3. 对任意 $g\in G$，$gHg^{-1}\subseteq H$。

4. 对任意 $g\in G$，$h\in H$，$ghg^{-1}\in H$。

证明的思路是 1=>2=>3=>4=>1。

1=>2，因为对任意的 $g\in G$，都有 $gH=Hg$，因此 $gHg^{-1}=(gH)g^{-1}=(Hg)g^{-1}=H(gg^{-1})=He=H$。

2=>3 因为对任意的 $g\in G$，$gHg^{-1}=H$，显然包含关系也成立，即 $gHg^{-1}\subseteq H$。

3=>4 由于$gHg^{-1}\subseteq H$，因此对任意$g\in G,h\in H$，都有$ghg^{-1}\in H$。

4=>1 由于$ghg^{-1}\in H$，因此对任意$h\in H$，都存在$h_1\in H$，满足$ghg^{-1}=h_1$，亦即$gh=h_1g\in Hg$，由于h的任意性，故$gH\subseteq Hg$；反之，任取$g^{-1}\in G$，有$g^{-1}h(g^{-1})^{-1}\in H$，即$g^{-1}hg\in H$，故存在$h_2\in H$，满足$g^{-1}hg=h_2$，亦即$hg=gh_2\in gH$，因此$Hg\subseteq gH$，综上有$gH=Hg$，对任意的$g\in G$。

在以上几个判别正规子群的方法中，一般性质4使用更经常些，因为它只需要判别ghg^{-1}是否在H中，而无需顾及两个子集是否相等。

例 8.6.5 设G是全体$n\times n$阶实可逆矩阵关于矩阵乘法作成的群，H是G中全体行列式值为1的矩阵集合，则H是G的子群，而且是正规子群，因为对任意的$A\in G$，$B\in H$，有

$$|ABA^{-1}|=|A||B||A^{-1}|=|A||B|\frac{1}{|A|}=|B|=1。$$

所以$ABA^{-1}\in H$，即$H\lhd G$。

例 8.6.6 若G的一个子群H的任意两个左陪集的乘积仍然是H的一个左陪集，则H是G的一个正规子群。

证明：设aH,bH是H的任意两个左陪集，令$aH\cdot bH=cH$，由于$ab=(ae)(be)\in aHbH=cH$，因此$ab\in cH$，亦即$abH=cH$，所以$aH\cdot bH=abH$。

任取$h\in H$，且对任意$g\in G$，$ghg^{-1}h\in gHg^{-1}H=(gg^{-1})H=H$，所以$ghg^{-1}\in H$，亦即$H\lhd G$。

在Lagrange定理的推论3中曾经定义了群G的两个子群的乘积，即设，$A,B\leqslant G$，则$AB=\{ab|a\in A,b\in B\}$，一般说来AB不一定是G的子群，但是如果A,B之中至少有一个是正规子群的话，可以得到下述定理。

定理 8.6.2 设A,B是G的两个子群

1. 若$A\lhd G,B\lhd G$，则$A\cap B\lhd G,AB\lhd G$。

2. 若$A\lhd G,B\leqslant G$，则$A\cap B\lhd B,AB\leqslant G$。

证明：任取$h\in A\cap B$，于是$h\in A,h\in B$，对任意的$g\in G$，由于A,B都是正规子群，因此$ghg^{-1}\in A,ghg^{-1}\in B$,，故$ghg^{-1}\in A\cap B$，即$A\cap B\lhd G$。对任意$a\in A,b\in B$，有$ab\in AB$，任取$g\in G$，有$gag^{-1}\in A,gbg^{-1}\in B$，于是$(gag^{-1})(gbg^{-1})\in AB=ga(g^{-1}g)bg^{-1}\in AB=g(ab)g^{-1}\in AB$，因此$AB\lhd G$。下面证明第二部分，因为$A\lhd G,B\leqslant G$，所以$e\in A\cap B\neq\phi$，且对任意$h\in A\cap B$以及$b\in B$，有$bhb^{-1}\in B$，同时因为$b\in G,h\in A\lhd G$，所以$bhb^{-1}\in A$，故$bhb^{-1}\in A\cap B$，因此$A\cap B\lhd B$。由$A\lhd G$知，对任意$g\in G$，有$gA=Ag$。亦即任取$a\in A$，一定有$a'\in A$，满足$ga=a'g$。这样任取$ab,a_1b_1\in AB$，$(ab)(a_1b_1)=a(ba_1)b_1=a(a_1'b)b_1=(aa_1')(bb_1)\in AB$，即$AB$关于乘法运算是封闭的，又由于$e\in AB$，以及$(ab)^{-1}=b^{-1}a^{-1}=(a^{-1})'b^{-1}\in AB$，因此$AB\leqslant G$。

定理 8.6.3 设H是G的一个正规子群，G/H表示H的所有陪集构成的集合，则G/H关于陪集乘法作成群。称之为G关于H的商群。

证明：首先证陪集乘法是G/H中的一个二元运算，对任的$aH,bH\in G/H$，$aHbH=\{ah_1bh_2|h_1,h_2\in H\}$，由于$bH=Hb$，因此$ah_1bh_2=a(h_1b)h_2=a(bh_1')h_2=(ab)(h_1'h_2)=$

$abh' \in abH$，其中 $h'_1, h' \in H$。因为 h_1, h_2 的任意性，所以 $aHbH \subseteq abH$；同时对任意的 $h \in H$，$(ab)h \in abH$，由于 $(ab)h=(ae)(bh) \in aHbH$，所以 $abH \subseteq aHbH$，因此 $aHbH=abH$，而 $abH \in G/H$，所以 G/H 对乘法是封闭的。

对任意的 $aH, bH, cH \in G/H$，$(aHbH)cH=(abH)cH=(ab)cH=a(bc)H=aH(bcH)=aH(bHcH)$，所以 G/H 对该运算适合结合律。又由于 $eHaH=eaH=aH$，$aHeH=aeH=aH$，所以有单位元 $eH=H$。而且 aH 的逆元是 $a^{-1}H$，因此 G/H 关于陪乘法构成群。

例 8.6.7 设 $G=S_3$，$H=\{(1),(123),(132)\}$，G/H 含有二个元素，即 $G/H=\{H,(12)H\}$，其乘法表是：

$\cdot$	H	$(12)H$
H	H	$(12)H$
$(12)H$	$(12)H$	H

显见 G/H 是群。

例 8.6.8 设 $(Z,+,0)$ 是整数加群，$nZ=\{nk \mid k \in Z\}$ 是 Z 的一个子群，其中 n 是正整数，因为 Z 是交换群，所以 nZ 是正规子群。商群 Z/nZ 是由 nZ 的全部陪集构成的。nZ 在 Z 中的全部陪集是

$$nZ, 1+nZ, \cdots, (n-1)+nZ。$$

在商群 Z/nZ 中的运算是

$$(i+nZ)+(j+nZ)=(i+j)+nZ=r+nZ,$$

其中 $r \equiv i+j \pmod n$，由此可见 Z/n 与剩余类加群 $Zn=\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ 完全是一致的，亦即整数加群对 nZ 的商群就是整数模 n 的剩余类加群。

由于商群 G/H 是 H 在 G 中全部陪集的集合，而且其陪集个数（指数）是 $[G:H]$，所以该商群的阶就是 $[G:H]$。当 G 是有限群时，G/H 也是有限群，且 $[G:H]=|G|/|H|$；若 G 是无限群，但 H 在 G 中的指数有限时，G/H 也是有限群。

8.7 群的同态、同态基本定理

如同一般代数系统的同态与同构的关系一样，群的同态是同构的引伸和推广。

定义 8.7.1 设 G_1, G_2 是两个群，f 是 G_1 到 G_2 的一个映射。如果对任意的 $a, b \in G_1$，都有

$$f(ab)=f(a)f(b),$$

则称 f 是 G_1 到 G_2 的一个同态映射，或简称同态。

若 f 分别是单射，满射和双射时，分称之为单一同态、满同态和同构。用 $G_1 \sim G_2$ 表示满同态，并称 G_2 是 f 作用下 G_1 的同态象。

由定义可知，群的同构既是单一同态又是满同态，因此它是一种特殊的同态映射。

例 8.7.1 设 G, G' 是两个群，令 $f: x \to e'$，对任意 $x \in G$。此处 e' 是 G' 的单位元，则 f 是 $G \to G'$ 的映射，而且对任意 $x, y \in G$，$f(xy)=e'=e'e'=f(x)f(y)$，所以 f 是 G 到 G' 的

一个同态，这个同态在任何两个群之间都存在，一般称之为零同态。

例 8.7.2 设 $G_1=(Z,+,0)$，$G_2=(Z_n,+,0)$，定义 $f:a\to\bar{r}$ 其中 $a=pn+r$。$0\leqslant r<n$，$a\in G_1$，则 f 是 G_1 到 G_2 的一个满同态。

证明：对任意 $a\in Z$，都有唯一余数 r，使 $\bar{r}\in Zn$，即 $f(a)\in Zn$，因此 f 是 G_1 到 G_2 的一个映射。同时对任意 $\bar{r}\in Zn(0\leqslant r<n)$，都存在 $a\in G_1$，满足 $a=pn+r$（p 是整数），使 $f(a)=\bar{r}$，所以 f 是满射。又由于对任意的 $a,b\in G_1$，

$$f(a+b)=\overline{a+b}=\bar{a}+\bar{b}=f(a)+f(b)。$$

因此 f 是 G_1 到 G_2 的满同态，即 $G_1\sim G_2$。

例 8.7.3 设 H 是 G 的正规子群，对任意 $a\in G$，令 $f:a\to aH$，则 f 是 G 到 G/H 的满同态。

证明：显然 f 是 G 到 G/H 的一个映射，因为对任意 $a\in G$，都有 $f(a)=aH\in G/H$；同时对任意 $aH\in G/H$，都存在有 $a\in G$，满足 $f(a)=aH$，因此 f 是 G 到 G/H 的一个满射。又由于

$$f(ab)=abH=aHbH=f(a)f(b)。$$

所以 f 是 G 到 G/H 的满同态。

这个同态也称为 G 到其商群 G/H 的自然同态，因此 G 的商群是 G 的同态象。

定理 8.7.1 若 f 是 G_1 到 G_2 的同态，g 是 G_2 到 G_3 的同态，则 gf 是 G_1 到 G_3 的同态。

证明：显然 gf 是 G_1 到 G_3 的映射，以下只证明它保持运算，对任意 $a,b\in G_1$

$$\begin{aligned}gf(ab)&=g(f(ab))=g(f(a)f(b))=g(f(a))g(f(b))\\&=gf(a)gf(b)。\end{aligned}$$

因此 gf 是 G_1 到 G_3 的同态。

群的同态还具有下述性质。

定理 8.7.2 设 G 是一个群，$(G',\cdot)$ 是一个有二元运算的代数系统，若 $f:G\to G'$ 是满射，且保持运算，则 G' 也是群，而且 $G\sim G'$。

证明留给读者作为练习。

定理 8.7.3 设 f 是 G 到 G' 的同态，则

1. 若 e 和 e' 分别是 G 和 G' 的单位元，则 $f(e)=e'$。

2. 对任意 $a\in G$，f 将 a 的逆元映射到 G' 中 $f(a)$ 的逆元，即 $f(a^{-1})=f^{-1}(a)$。

3. 如果 H 是 G 的子群，则 H 在 f 下的象 $f(H)=\{f(a)\mid a\in H\}$ 是 G' 的子群，而且 $H\sim f(H)$。

证明：

1. $f:G\to G'$ 是同态，即取 $a,b\in G$，$f(ab)=f(a)f(b)$，所以 $f(ea)=f(e)f(a)=f(ae)$，即 $f(e)$ 是 G' 中的单位元，$f(e)=e'$。

2. 任取 $a\in G$，有 $a^{-1}\in G$，$f(aa^{-1})=f(e)=e'=f(a)f(a^{-1})$，$f(a^{-1}a)=f(e)=e'=f(a^{-1})f(a)$。故 $f^{-1}(a)=f(a^{-1})$。

3. 任取 $a,b\in H$，则 $f(a),f(b)\in f(H)$，由于 $H\leqslant G$，故 $ab\in H$，亦即 $f(ab)\in f(H)$，因为 f 是同态，所以 $f(ab)=f(a)f(b)$，即 $f(a)f(b)\in f(H)$，也就是说 $f(H)$ 是封闭的；

又因 $e\in H$，故 $f(e)\in f(H)$，由于 $ea=ae=a$，所以 $f(ea)=f(e)f(a)=f(a)f(e)=f(a)$，即 $f(e)$ 是 $f(H)$ 的单位元。再者，对任意 $a\in H$，都有 $a^{-1}\in H$，所以 $f(a^{-1})\in f(H)$，由于 $f(a)f(a^{-1})=f(aa^{-1})=f(e)$，$f(a^{-1})f(a)=f(a^{-1}a)=f(e)$，故 $f(a^{-1})$ 是 $f(a)$ 的逆元，因此 $f(H)$ 是一个群，且 $f(H)\leqslant G'$。

对任意 $a\in H$，都有唯一的 $f(a)\in f(H)$，对任意 $f(x)\in f(H)$，都存在有 $x'\in H$，满足 $f(x')=f(x)$，因此 f 是 H 到 $f(H)$ 的满射，故 $H\sim f(H)$。

设 f 和 g 都是 G 到 G' 的同态，怎样确定 f 和 g 是相等的呢？除了一一判断 G 中的每个元素 x，都有 $f(x)=g(x)$ 以外，再介绍一个定理。

定理 8.7.4 设 f 和 g 都是 G 到 G' 的同态，S 是 G 的生成元集，假定对任意的 $s\in S$，都有 $f(s)=g(s)$，则 $f=g$。

证明：令 $G_1=\{a\in G\mid f(a)=g(a)\}$，因为 $f(e)=e'=g(e)$，所以 $e\in G_1$，因此 G_1 非空且 $G_1\supseteq S$。同时若 $a,b\in G_1$，则 $f(ab)=f(a)f(b)=g(a)g(b)=g(ab)$，因此 $ab\in G_1$，且若 $a\in G_1$，有 $f(a^{-1})=f^{-1}(a)=g^{-1}(a)=g(a^{-1})$，即 $a^{-1}\in G_1$，因此 G_1 是 G 的子群，由于 $G_1\supseteq S$，并根据生成元集合 S 的定义，因此 $G_1=G$，于是对所有 $a\in G$，都满足 $f(a)=g(a)$，即 $f=g$。

下面介绍同态核的概念及性质。

定理 8.7.5 设 f 是 G 到 G' 的同态，e 是 G 的单位元，令 $K=\{a\in G\mid f(a)=f(e)\}$，则 K 是 G 的正规子群，K 称为同态 f 的核，记作 $\mathrm{Ker}f$。

证明：由于 f 是同态，所以 $f(e)=e'$ 是 G' 的单位元。设 $k,k_1\in K$，有 $f(kk_1)=f(k)f(k_1)=f(e)f(e)=e'=f(e)$，且 $f(k^{-1})=f^{-1}(k)=f^{-1}(e)=e'=f(e)$，所以 $k^{-1}\in K$，因此 K 是 G 的子群。对任意 $g\in G,k\in K$，因为

$$f(g^{-1}kg)=f(g^{-1})f(k)f(g)=f^{-1}(g)f(k)f(g)$$
$$=f^{-1}(g)f(g)=e'=f(e),$$

因此 $g^{-1}kg\in K$，故 K 是 G 的正规子群。

定理 8.7.6 设 f 是 G 到 G' 的同态，K 是同态的核，那么对任意的 $a,b\in G$，$f(a)=f(b)$ 的充要条件是 $b\in aK$。

证明：充分性。由于 $b\in aK$，所以存在一个 $k\in K$，满足 $b=ak$，因此 $f(b)=f(ak)=f(a)f(k)=f(a)f(e)=f(a)$。必要性，因为 $f(a)=f(b)$，所以 $f^{-1}(a)f(a)=f^{-1}(a)f(b)=f(a^{-1})f(b)=f(a^{-1}b)=e'=f(e)$，亦即 $a^{-1}b\in K$ 或 $b\in aK$。

对于 G 到 G' 的任何同态 f，都可以得到 G 的一个正规子群——同态核 $\mathrm{Ker}f$，$\mathrm{Ker}f$ 中至少包含 G 中的单位元 e。利用同态核能够判断一个同态是否为单同态。

定理 8.7.7 设 f 是 G 到 G' 的一个同态，则 f 是单同态的充要条件是 $\mathrm{Ker}f=\{e\}$。

证明：设 f 是单同态，则 f 是 G 到 G' 的一个单射，所以 G' 中的单位元 e' 在 G 中只有一个原象 e，因此 $\mathrm{Ker}f=\{e\}$。再证充分性，对任意 $a,b\in G$，且 $f(a)=f(b)$，则 $f(a)f^{-1}(b)=f(a)f(b^{-1})=f(ab^{-1})$。而 $f(a)f^{-1}(b)=f(b)f^{-1}(b)=f(b)f(b^{-1})=f(bb^{-1})=f(e)$，故 $ab^{-1}=e$，亦即 $a=b$。因此 f 是单同态。

从该定理可以得到如下推论：

推论：设 f 是从 G 到 G' 的满同态，则 f 为同构的充要条件是 $\mathrm{Ker}f=\{e\}$。

8.6 节已指出，任取 G 的一个正规子群 H，则对应存在由 H 的陪集构成的商群 G/H，那么 G 和其商群 G/H 之间的关系如何呢？对此我们有

同态基本定理：设 G 是一个群，则 G 的任一商群都是 G 的同态象；反之，若 G' 是 G 的同态象，f 是 G 到 G' 的满同态，则 $G' \cong G/K$，其中 $K = \mathrm{Ker} f$。

证明：设 G/H 是 G 的任一商群，显然 $H \lhd G$，对任意的 $a \in G$，令 $g: a \to aH$，由例 8.7.3可知 g 是 G 到 G/H 的满同态，即 G/H 是 G 的一个同态象。下面再证第二部分。设 f 是 G 到 G' 的满同态，$\mathrm{Ker} f = K$。令 $\varphi: aK \to f(a)$，对任意的 $aK \in G/K$，我们要证明 φ 是 G/K 到 G' 的同构映射。

首先，对任意 $aK = bK$，都有 $a^{-1}b \in K$，所以 $f(a^{-1}b) = f(e)$，亦即 $f(a) = f(b)$，也就是说 $\varphi(aK) = \varphi(bK)$，因此 φ 是 G/K 到 G' 的映射。其次，对任意 $x \in G'$，由于 f 是满同态，可知存在有 $a \in G$，使 $f(a) = x$，因此 $\varphi(ak) = f(a) = x$，即 φ 是 G/K 到 G' 的满射。同时由于

$$\begin{aligned}\varphi(aKbK) &= \varphi(abK) = f(ab) = f(a)f(b) \\ &= \varphi(aK)\varphi(bK),\end{aligned}$$

因此 φ 是 G/H 到 G' 的满同态。最后，由于 K 是 f 的同态核，根据定义 $f(a) = f(e) <=> a \in K$，有

$$\begin{aligned}\mathrm{Ker}\varphi &= \{aK \in G/K \mid \varphi(aK) = \varphi(K)\} \\ &= \{aK \mid f(a) = f(e)\} = \{K\}。\end{aligned}$$

根据定理 8.7.7 知 φ 是单同态。所以 φ 是 G/K 到 G' 的同构，即 $G/K \cong G'$。

同态基本定理表明，G 的任一商群都是 G 的一个同态象，同时 G 的任一同态象都与 G 的某个商群同构。因此在同构的意义下，G 的任一同态象不过是 G 的某个商群而已，所以若把 G 的每个商群决定以后，它的所有同态象都随之而定。

例 8.7.4　设 H 是 G 的正规子群，$f: G \to G/H$ 是自然同态，求 $\mathrm{Ker} f$。

因为 f 是自然同态，所以对任意 $a \in G$，有 $f(a) = aH$，根据定义 $\mathrm{Ker} f = \{a \in H \mid f(a) = f(e)\} = \{a \in G \mid aH = H\}$，显然 $\mathrm{Ker} f = H$。

例 8.7.5　设 G 和 G' 分别是阶数为 m 和 n 的循环群 $(m \geqslant n)$，则 $G \sim G'$ 的充要条件是 $n \mid m$。

证明：若 $G \sim G'$，由同态基本定理得知 G' 同构于的一个商群 G/K，其中 $K = \mathrm{Ker} f$。f 是 G 到 G' 的满同态，因此 $|G'| = n = |G/K|$，由于商群 G/K 的阶是 $[G:K] = |G|/|K|$，所以 $n = m/|K|$，$|K|$ 是正整数，故 $n \mid m$。反之，设 $n \mid m$，令 $G = \langle a \rangle$，$G' = \langle b \rangle$，规定 G 到 G' 的映射 $f: a^k \to b^k$，对 $\langle a \rangle$ 中的任意 a^k, a^l，若 $a^k = a^l => a^{k-l} = e => m \mid k-l => n \mid k-l => b^{k-l} = e => b^k = b^l$。这就是说，对于 G 中的任一元，无论其表示方法如何，在 f 下有唯一的象，所以 f 是映射，而且对任意 $b^r \in G'$，都有 $a^r \in G$，使 $f(a^r) = b^r$，故 f 是满射；再者，对任意 $a^i, a^j \in G$，$f(a^i a^j) = f(a^{ij}) = b^{i+j} = b^i b^j = f(a^i) f(a^j)$，所以 f 是满同态，即 $G \sim G'$。

假定 G' 是 G 的同态象，则同态核 $\mathrm{Ker} f$ 是 G 的正规子群，G 中也一定存在包含 $\mathrm{Ker} f$ 的子群。我们现在分析这些子群与 G' 的诸子群之间的关系。

定理 8.7.8　设 K 是 G 的正规子群，H 是 G 中包含 K 的子群，则

1. $H'=H/K$ 是 $G'=G/K$ 的子群。

2. $\varphi: H \to H'$ 是 G 中包含 K 的子群的集合到 G' 的子群的集合之间的双射。

3. H 是 G 的正规子群的充要条件是 H' 是 G' 的正规子群，而且此时

$$G/H \cong G'/H' = \frac{G/K}{H/K}。$$

证明：由于 H 是 G 的子群，且包含 K，因此 K 亦是 H 的正规子群。由商群的定义，H/K 自然是 G/K 的子群。下面证明 $\varphi: H \to H'$ 是双射。令 H_1, H_2 是两个包含 K 的 G 的子群，假定 $H_1/K=H_2/K$，则对任意的 $h_1 \in H_1$，有 $h_1K \in H_1/K$ 亦即 $h_1K \in H_2/K$，这样，存在某个 $h_2 \in H_2$ 满足 $h_1K=h_2K$，由陪集性质，$h_2^{-1}h_1 \in K$，因此存在 $k \in K$ 满足 $h_1=h_2k$，由于 $K \lhd H_2$，所以 $k \in H_2$，亦即 $h_1 \in H_2$，故 $H_1 \subseteq H_2$。同理 $H_2 \subseteq H_1$，因此 $H_1=H_2$，这说明 $\varphi: H \to H'$ 是单射，再证 φ 是满射。令 H' 是 $G'=G/K$ 的任一子群，由于 G' 实际上是 G 中关于子群 K 的全部陪集的集合。因此 H' 是其中某些陪集的集合。令 H 是 G 中这些陪集的并，现在我们证明 H 是 G 的一个子群。假定任意的 $h_1, h_2 \in H$，则 $h_1K, h_2K \in H'$，这样有 $h_1h_2K=(h_1K)(h_2k) \in H'$，因此 $h_1h_2 \in H$，故 H 是封闭的；同时 H 中有单位元 e，另外由于 H' 是子群，所以任一 $h_1K \in H'$ 都有逆元 $(h_1K)^{-1} \in H'$，由于 $(h_1K)(h_1^{-1})=h_1h_1^{-1}K=K$，故 $h_1^{-1}K=(h_1K)^{-1} \in H'$，所以 $h_1^{-1} \in H$，因此 h_1 在 H 中有逆元 h_1^{-1}，从而 H 是 G 的子群。因此 φ 是满射，第二部分得证。

以下再证明定理的第三部分。由于 $H'=H/K=\{hK \mid h \in H\}$，所以对任意 $gK \in G'$，$hK \in H'$，有 $(gK)(hK)(gK)^{-1}=(ghg^{-1})K$，由于 $H \lhd G$，所以 $ghg^{-1}=h' \in H$，故 $(ghg^{-1})K=h'K \in H'$，即 H' 是 G' 的正规子群。反之，若 $H' \lhd G'$，则对任意 $g \in G, h \in H$，$(ghg^{-1})K=(gK)(hK)(g^{-1}K)=(gk)(hK)(gk)^{-1} \in H'$，因此 $ghg^{-1} \in H$，即 $H \lhd G$。这时我们可以构造一个商群 G'/H'，且存在一个自然同态 $f': G' \to G'/H'$，使得对 G' 中的任意元素 $\bar{g}$，有 $f'(\bar{g})=\bar{g}H$；同时 G 到 G' 也有一个自然同态 $f: g \to \bar{g}$。于是可以得到从 G 到 G'/H' 的一个满同态 φ，该同态的核是满足 $\bar{g} \in H'$ 的所有 $g \in G$ 的集合，由于 $H'=\{hK \mid h \in H\}$，且 $K \lhd H$，所以该集合就是 H 本身，亦即。$\mathrm{Ker}\varphi=H$。由同态基本定理，$G/H \cong G'/H'$。

定理 8.7.9 令 H 和 K 是 G 的子群，且 K 是正规子群，则映射 $f: hK \to h(K \cap H)$，$h \in H$，是 HK/K 到 $H/(K \cap H)$ 的一个同构。

证明：由定理 8.6.2 知 $K \cap H$ 是 H 的正规子群，HK 是 G 的子群，且因 $K \subseteq HK$，所以 K 是 HK 的正规子群，因此存在商群 HK/K 和 $H/(K \cap H)$。下面证明它们之间存在同构。设 $f: g \to gK, g \in H$，则 f 的象是所有 $h \in H$ 的陪集 hK 的集合。由于任何陪集 hkK，其中 $h \in H, k \in k$，都与 hK 是一致的，所以 f 的象就是 HK/K，该同态的核就是满足 $hK=K$ 的 $h(\in H)$ 的集合，亦即它是 HK/K 中的单位元。因为 $hK=K$ 的充要条件是 $h \in K$，所以 $\mathrm{Ker}f=H \cap K$，由同态基本定理，$H/(H \cap K)$ 与 HK/K 同构。

例 8.7.6 设 H 是 G 的正规子群，$|G|=mn$，$|H|=n$，且 m 与 n 互素，则 H 是 G 的唯一一个阶为 n 的子群。

证明：设 H' 是 G 的另一个 n 阶子群，则 $H'H$ 是 G 的含有 H 的子群，因此 $H'H/H$ 是 G/H 的子群，由于 $|G/H|=m$，设 $H'H/H$ 的阶为 k，则 $k \mid m$。由定理 8.7.9 有 $H'H/$

$H \cong H'/(H' \cap H)$，因此 $H'/(H' \cap H)$ 的阶也是 k，但 H' 的阶是 n，故 $k|n$。由于 k 是 m 和 n 的因子，且 m 与 n 互素，故 $k=1$，因此 $H'H=H$，即 $H'=H$，所以 H 是唯一的 n 阶子群。

8.8 群的直积

定义 8.8.1 设 G_1, G_2 是两个群，它们的积代数 $G_1 \times G_2$ 关于乘法 $(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2)$ 作成的群叫做 G_1, G_2 的直积，用 $G_1 \times G_2$ 表示。

如果 G_1, G_2 是有限群，那么 $G_1 \times G_2$ 也是有限群，而且 $|G_1 \times G_2| = |G_1||G_2|$。如果 G_1, G_2 都是可交换群，则 $(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2)=(a_2a_1,b_2b_1)=(a_2,b_2)(a_1,b_1)$，亦即 $G_1 \times G_2$ 也是可交换群。

例 8.8.1 设 $G=\{e,a\}$ 是二阶循环群，则 $G \times G$ 有 4 个元素，即 $G \times G=\{(e,e),(e,a),(a,e),(a,a)\}$，由于除单位元 (e,e) 外其余元素的阶都是 2，所以它与 Klein 四元群同构。

例 8.8.2 设 $G_1=\langle a\rangle$ 是 r 阶循环群。$G_2=\langle b\rangle$ 是 s 阶循环群，若 r 与 s 互素，则 $G_1 \times G_2$ 是 rs 阶循环群。

证明：(a,b) 是 $G_1 \times G_2$ 的一个元，由 $\langle(a,b)\rangle$ 可以构成 $G_1 \times G_2$ 的一个子群，设它的阶为 d，因为 $(a,b)^{rs}=(a^{rs},b^{rs})=(e_1,e_2)$，故 $d|rs$。同时由于 $(a,b)^d=(a^d,b^d)=(e_1,e_2)$，所以 $r|d, s|d$，亦即 $[r,s]|d$，而 r 与 s 互素，故 $rs|d$。因此 $rs=d$。由于 $G_1 \times G_2$ 是 rs 阶的群，而 $\langle(a,b)\rangle$ 的阶也是 rs，所以 (a,b) 是 $G_1 \times G_2$ 的一个生成元，$G_1 \times G_2$ 是循环群。

例 8.8.3 设 H_1, H_2 分别是 G_1, G_2 的正规子群，则 $H_1 \times H_2$ 是 $G_1 \times G_2$ 的正规子群。

证明：易见 $H_1 \times H_2$ 是 $G_1 \times G_2$ 的子群。设 $(a,b) \in H_1 \times H_2$，对任意的 $x \in G_1, y \in G_2$，$(x,y) \in G_1 \times G_2$，有 $(x,y)(a,b)(x,y)^{-1}=(x,y)(a,b)(x^{-1},y^{-1})=(xax^{-1},yby^{-1})$，因为 H_1, H_2 是正规子群，所以 $xax^{-1} \in H_1, yby^{-1} \in H_2$，故 $(xax^{-1},yby^{-1}) \in H_1 \times H_2$，$H_1 \times H_2 \lhd G_1 \times G_2$。

定理 8.8.1 设 G_1, G_2 是 G 的两个正规子群，若 G 中的每个元可以唯一地用 G_1, G_2 的元的积来表示，则 $G \cong G_1 \times G_2$。

证明：由定理 8.6.2，G_1G_2 是 G 的正规子群，由于对任意 $g \in G$，都有 $g=g_1g_2$，其中 $g_1 \in G_1, g_2 \in G_2$，而且该表示是唯一的。这样，设 $f: g_1g_2 \to (g_1,g_2)$，易证 f 是 G_1G_2 到 $G_1 \times G_2$ 的双射。要证明 f 保持运算，需要先证对任意的 $g_1 \in G_1, g_2 \in G_2$，均有 $g_1g_2=g_2g_1$。由于 G 的元可以唯一地用 G_1G_2 中的元素表示，故 $G_1 \cap G_2=e$，否则若 $g \in G_1 \cap G_2$，则 $g=ge=eg$，g 的表示法不唯一，产生矛盾。由于 $(g_1g_2)(g_2g_1)^{-1}=g_1g_2g_1^{-1}g_2^{-1}=(g_1g_2g_1^{-1})g_2^{-1} \in G_2$，$(g_1g_2)(g_2g_1)^{-1}=g_1g_2g_1^{-1}g_2^{-1}=g_1(g_2g_1^{-1}g_2^{-1}) \in G_1$，所以 $(g_1g_2)(g_2g_1)^{-1} \in G_1 \cap G_2$，即 $g_1g_2(g_2g_1)^{-1}=e$，$g_1g_2=g_2g_1$，这样

$$
\begin{aligned}
f((g_1g_2)(g_1'g_2')) &= f(g_1(g_2g_1')g_2') \\
&= f(g_1g_1'g_2g_2') = f((g_1g_1')(g_2g_2')) \\
&= (g_1g_1', g_2g_2') = (g_1,g_2)(g_1',g_2') \\
&= f(g_1g_2)f(g_1'g_2')。
\end{aligned}
$$

因此 f 是 G 到 $G_1 \times G_2$ 的同构。

这个定理说明，如果 G_1,G_2 是 G 的正规子群，且 G 的每个元都可以唯一地用 G_1,G_2 中的元的乘积表示，则 G 可以用 G_1 和 G_2 的直积表示。这时我们也称 G 是其子群 G_1,G_2 的内部直积。

直积的概念也可以推广到 n 个群的情形。

定义 8.8.2 设 $G_1,G_2,\cdots,G_n$ 是 n 个群，在 $G=G_1 \times G_2 \times \cdots \times G_n$ 中定义，对任意的 a，$b \in G$，$a=(g_1,g_2,\cdots,g_n)$，$b=(g_1',g_2',\cdots,g_n')$ 有

$$
\begin{aligned}
ab &= (g_1,g_2,\cdots,g_n)(g_1',g_2',\cdots,g_n') \\
&= (g_1g_1',g_2g_2',\cdots,g_ng_n')。
\end{aligned}
$$

则 G 关于上述运算构成群，称之为 $G_1,G_2,\cdots,G_n$ 的直积。

显然群 G 中的单位元是 $(e_1,e_2,\cdots,e_n)$，对其中的任意元 $(g_1,g_2,\cdots,g_n)$，都有其逆元 $(g_1,g_2,\cdots,g_n)^{-1}=(g_1^{-1},g_2^{-1},\cdots,g_n^{-1})$。如果 $G_1,G_2,\cdots,G_n$ 都是有限群，设 $G_i(i=1,2,\cdots,n)$ 的阶是 $|G_i|$，则直积 G 也是有限群，且它的阶是 $|G| = \prod_{i=1}^{n} |G_i|$。而且如果 G_i 都是可交换群，则 G 也是可交换群。

定理 8.8.2 设 G 有 n 个正规子群 G_i，$i=1,2,\cdots,n$，若 G 中的每个元都可以唯一地用 $G_1,G_2,\cdots,G_n$ 中的元的积来表示，则 $G \cong G_1 \times G_2 \times \cdots \times G_n$。

该定理的证明思路与前一定理类似，留给读者作为练习。

习 题 八

1. 在实数集 R 中定义运算・如下：$a \cdot b=a+b+ab$，对任意 $a,b \in R$，证明：

   a）$(R,\cdot)$是半群。

   b）$(R,\cdot)$是幺群。

   c）找出$(R,\cdot)$中全部可逆元。

2. 设$(S,\cdot)$是半群，证明 $S \times S$ 对于下面规定的结合法・作成一个半群

$$(a_1,a_2)\cdot(b_1,b_2) = (a_1\cdot b_1,a_2\cdot b_2),$$

当 S 有单位元时，$S \times S$ 也有单位元。

3. 设$(S,\cdot)$是半群，且左、右消去律都成立，证明 S 是交换半群的充要条件是对任意 $a,b \in S$，

$$(ab)^2 = a^2b^2。$$

4. 设 Z 是整数集，$\times$ 表示乘法运算，试证明$(Z,\times)$是幺群，且$(\{O\},\times)$是子半群而不是子幺群。

5. 证明定理 8.1.3 的推论。

6. 设 σ 是幺群$(S,\cdot)$到$(T,*)$的同构，证明如果 e 是 S 的单位元，则 $\sigma(e)$是$(T,*)$的单位元。

7. 设 G 是群，证明如果 G 中任意元的逆元都是它自身，则 G 是交换群。

8. 令 $G=\{km \mid k \in Z\}$，m 是取定的自然数，证明$(G,+)$是群。

9. 设$G=(Z,\cdot)$，对任意的$a,b\in Z$，规定

$$a\cdot b=a+b-2,$$

证明G是群。

10. 设G是群，$a,b,c\in G$，证明

$$xaxba=xbc$$

在G中有且仅有一个解。

11. 令G是实数对(a,b)的集合，$a\neq 0$，定义

$$(a,b)(c,d)=(ac,cd+b)$$

以及单位元$e=(1,0)$，证明G是群。

12. 设G是幺群，$a,b\in G$，证明a有可逆元b的充要条件是$aba=a$和$ab^2a=e$。

13. 设H是G的子群，$x\in G$，令

$$H_1=x^{-1}Hx=\{x^{-1}hx\mid h\in H\},$$

证明H_1是G的子群。

14. 证明G中多个子群的交仍然是G的子群。

15. 说明 Klein 四元群是否为循环群。

16. 求剩余类加群$(z_{100},+)$的所有子群。

17. 设G是阶为素数p的循环群，则G的任意元$a(a\neq e)$都是G的生成元。

18. 证明整数加群$(z,+)$与偶数加群同构。

19. 证明若群G除单位元以外，其余每个元的阶都是2，则G是交换群。

20. 设$G=\langle a\rangle$，$G_1=\langle a^r\rangle$，$G_2=\langle a^s\rangle$分别是G的子群，其中r、s是非负整数，证明$G_1\cap G_2=\langle a^d\rangle$，其中$d=[r,s]$。

21. 在S_6中设

$$\sigma=\begin{bmatrix}1&2&3&4&5&6\\4&3&5&6&1&2\end{bmatrix}\qquad \tau=\begin{bmatrix}1&2&3&4&5&6\\2&1&5&6&3&4\end{bmatrix}$$

试计算$\sigma\tau$、$\tau\sigma$、σ^{-1}、$\sigma\tau\sigma^{-1}$，同时将它们表成对换之积。

22. 求交错群A_4。

23. 设α是S_n中的任一置换，证明

$$\alpha(i_1,i_2,\cdots,i_r)\alpha^{-1}=(\alpha(i_1)\alpha(i_2)\cdots\alpha(i_r))。$$

24. 试证明S_n中的每个元都可以表成(1 2)、(1 3)、…、(1 n)这$n-1$个对换中若干个的乘积形式。

25. 证明任何一个偶数阶的有限群包含有元素$a\neq e$，满足$a^2=e$。

26. 证明任何一个群都不会是其二个真子群的并。

27. 设$\alpha=(1\ 3\ 2\ 4)$，试确定S_4中$\langle\alpha\rangle$的陪集。

28. 证明S_3的非平凡子群都是循环群，找出S_3的全部子群。

29. 设G是阶为6的群，证明G中一定有且只有一个3阶子群。

30. 令G是有限群，A、B是G的子群，并且$B\subseteq A$。证明

$$[G:B]=[G:A][A:B]$$

31. 设A、B是G的子群，证明AB是G的子群的充要条件是$AB=BA$。

32. 证明：e，(1 2)(3 4)，(1 3)(2 4)，(1 4)(2 3)四个置换群可构成群，而且是 S_4 的正规子群。

33. 设 H_1，H_2，H 是 G 的正规子群，且 $H_1 \subset H_2$，证明 H_1H 是 H_2H 的正规子群。

34. 设 G 是全体 $n \times n$ 阶实可逆矩阵乘法构成的群，H 是 G 中全体行列式值大于零的矩阵集合，证明 H 是 G 的正规子群。

35. 设 C 是 G 的中心，证明 C 的任何子群都是 G 的正规子群。

36. 设 G 是由实数对 (a,b) 构成的群，$a \neq 0$，$(a,b)(c,d) = (ac, ad+b)$，证明 $K = \{(1, b) \mid b \in R\}$ 是 G 的正规子群，且 $G/K \cong R^*$，R^* 是非零实数乘法群。

37. 设 $G = (R^*, \times)$ 是非零实数乘法群，判断以下哪些规则是 G 到 G 的同态映射。

$$f_1 : x \to x。$$

$$f_2 : x \to x^2。$$

$$f_3 : x \to \frac{1}{x}。$$

对于同态映射，找出 $f(G)$ 及 $\mathrm{Ker} f$。

38. 设 G 是循环群，H 是 G 的子群，证明 G/H 是循环群。

39. 设 f 是 G_1 到 G_2 的同态，g 是 G_2 到 G_3 的同态，证明 gf 是 G_1 到 G_3 的同态，且 gf 的核是 $f^{-1}g^{-1}(e'')$，其中 e'' 是 G_3 的单位元。

40. 证明对称群 S_4 对 Klein 四元群的商群与 S_3 同构，即 $S_4/K_4 \cong S_3$。

41. 设 G_1，G_2 是两个群，证明 $G_1 \times G_2$ 是交换群的充要条件是 G_1，G_2 都是交换群。

42. 设 G_1，G_2 是两个群，证明

$$G_1 \times G_2 \cong G_2 \times G_1。$$

第九章　环　和　域

第八章所讨论的是具有一个二元运算的代数系统，本章我们将介绍具有两个二元运算的代数系统：环和域。环是群的一种特定情况，它的不少内容与群有某些相似之处，在对环加某些限制之后就会得到域。

9.1　环及其性质

定义 9.1.1　给定一个代数系统$(R,+,\cdot)$，如果

1)$(R,+)$是交换群；

2)$(R,\cdot)$是半群；

3)对于运算+，运算·左、右分配律成立，即对任意的a、b、$c\in R$

$$a\cdot(b+c)=a\cdot b+a\cdot c,$$

$$(b+c)\cdot a=b\cdot a+c\cdot a。$$

则称代数系统R是一个环，其中+称为加法运算，·称为乘法运算。

通常称交换群$(R,+)$为加法群，其单位元为零元，用0表示，加法群中元素a的逆元记作$-a$，称为负元；同时称$(R,\cdot)$为乘法半群，如果它有单位元，则常称之为壹，用1表示。应该注意+和·不一定是普通的加法与乘法运算。

例 9.1.1　整数集Z对于数的加法和乘法作成一个环，称为整数环。

因为$(Z,+)$是个加法群，且是交换群，整数乘法适合结合律，故$(Z,\cdot)$是半群，再者乘法对加法满足分配律，所以$(Z,+,\cdot)$是一个环。

同理，有理数集Q，实数集R和复数集C关于加法和乘法运算也作成环$(Q,+,\cdot)$，$(R,+,\cdot)$和$(C,+,\cdot)$，它们都称为数环。

例 9.1.2　n阶的整数方阵的集合$(Z)_n$关于矩阵加法、乘法构成环。

显然$((Z)_n,+)$是交换群，$((Z)_n,\cdot)$是半群，而且对任意A、B、$C\in(Z)_n$

$$A(B+C)=AB+AC\ ,\ (B+C)A=BA+CA。$$

因此$(Z)_n$是环。

例 9.1.3　设Z_n表示模n的全体剩余类作成的集合，+表示模n的加法运算，其乘法运算规定为：对任意$\bar{a}$，$\bar{b}\in Z_n$；$\bar{a}\cdot\bar{b}=\overline{ab}$，则$(Z_n,+,\cdot)$作成环。

证明：显然$(Z_n,+)$是加法群，对任意$\bar{a}$，$\bar{b}\in Z_n$，规定$\bar{a}\,\bar{b}=\overline{ab}$，显然$\overline{ab}\in Z_n$，同时若有$\bar{a}_1=a$，$\bar{b}_1=b$，则一定存在整数$p$，$q$，满足$a_1=pn+a$，$b_1=qn+b$，从而

$$\overline{a_1b_1}=\overline{a_1b_1}=\overline{(pn+a)(qn+b)}=\overline{(pqn+aq+bp)n+ab}=\overline{ab}。$$

即二元运算·是封闭的，而且易证它适合结合律，所以$(Z_n,\cdot)$是半群。其次，对任意$\bar{a}$、$\bar{b}$，$\bar{c}\in Z_n$

$$\bar{a}(\bar{b}+\bar{c})=\bar{a}\,\overline{b+c}=\overline{a(b+c)}=\overline{ab+ac}$$

$$=\overline{ab}+\overline{ac}=\bar{a}\,\bar{b}+\bar{a}\,\bar{c}。$$

同理可证

$$(\bar{b}+\bar{c})\bar{a}=\bar{b}\,\bar{a}+\bar{c}\,\bar{a}。$$

即乘法对加法适合左、右分配律，所以$(Z_n,+,\cdot)$是环。

例 9.1.4 设$S=\{a,b,c\}$，S 中的加法和乘法运算如下表给出

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\cdot$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

则$(S,+,\cdot)$是环。

容易看出$(S,+)$是加法群，其中 a 是零元，b,c 互为负元。通过验证，$(S,\cdot)$是乘法半群，且 $\cdot$ 对$+$适合分配律，例如

$$b(b+c)=ba=a\ ,\ bb+bc=b+c=a。$$

例 9.1.5 设$(R,+)$是任一加法群，规定 R 上的乘法运算如下：对任意 $a,b\in R$，$ab=0$，则$(R,+,\cdot)$也是一个环，通常称之为零环。

下面我们讨论环的基本性质。以下 a,b,c 均为环 R 中的元素。

由于$(R,+)$是加法群，因此加法运算

1. 适合结合律，即$(a+b)+c=a+(b+c)$。

2. 适合交换律，即 $a+b=b+a$ 。

3. R 中存在一个零元 0，满足

$$a+0=a=0+a\ 。$$

4. 对任意 $a\in R$，a 有唯一负元$-a\in R$，满足 $a+(-a)=0=(-a)+a$，我们通常把 $a+(-b)$记为 $a-b$ 。

5. 满足消去律，即若 $a+b=a+c$，则 $b=c$ 。

6. 由于适合交换律，所以对任意整数 m,n，以下几个等式成立

$$n(a+b)=na+nb\ 。$$

$$(m+n)a=ma+na\ 。$$

$$mn(a)=m(na)\ 。$$

根据环的定义，我们知道乘法半群$(R,\cdot)$。

7. 适合结合律，即 $a(bc)=(ab)c$ 。

8. 对加法运算满足分配律，即 $a(b+c)=ab+ac$，$(b+c)a=ba+ca$。

其中性质 8 是重要的，因为它把两个不同的二元运算联系在一起了，否则它们将孤立地构成群与半群，我们也就不必去讨论具有两个二元运算的代数系统了。正是由于乘法对加法分配律的存在，我们可以推出以下性质：

9. 对任意 $a\in R$，$a\cdot 0=0=0\cdot a$ 。

因为 $a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0$，由性质 3，得到 $a\cdot 0=0$，同理 $0\cdot a=0$。

10. 对任意 $a,b\in R$，$(-a)b=a(-b)=-ab$ 。

因为 $ab+a(-b)=a(b+(-b))=a\cdot 0=0$，由性质 4 得到 $a(-b)=-ab$，同理可得

$(-a)b=-ab$。

11. 对任意 $a,b\in R$，$(-a)(-b)=ab$ 。

因为

$$a(-b)+(-a)(-b)=(a+(-a))(-b)=0\cdot(-b)=0\ ,$$

而 $a(-b)=-ab$，因此 $(-a)(-b)=ab$ 。

12. 乘法对减法的分配律成立，即对任意 $a,b,c\in R$，

$$a(b-c)=ab-ac\ ,\ (b-c)a=ba-ca。$$

证明：

$$a(b-c)=a(b+(-c))=ab+(-ac)=ab-ac\ 。$$

$$(b-c)a=(b+(-c))a=ba+(-ca)=ba-ca\ 。$$

13. 在环 R 中，乘法对加法的分配律可推广为

$$a(b_1+b_2+\cdots+b_n)=ab_1+ab_2+\cdots+ab_n$$

$$(b_1+b_2+\cdots+b_n)a=b_1a+b_2a+\cdots+b_na$$

$$\sum_{i=1}^{m}a_i\sum_{j=1}^{n}b_j=\sum_{i,j}a_ib_j$$

利用数学归纳法容易证明之。

14. 对任意 $a,b\in R$，n 是正整数，有

$$(na)b=a(nb)=nab\ 。$$

显见它是性质 13 的特例。

应该注意，因为 $(R,\cdot)$ 是半群，它不一定有单位元，每个元也不一定是可逆元，故乘法消去律在环中并不一定成立，因此若 $ab=0$，并不能推出 $a=0$ 或 $b=0$，从而在环中需要给出零因子的概念。

定义 9.1.2 设 R 是一个环，a,b 是 R 中两个非零元素，若 $ab=0$，则说 a 是 R 的一个左零因子，b 是 R 的一个右零因子，若 a 既是左零因子又是零因子，则称之为 R 的一个零因子。

注意零元不算是零因子。

例 9.1.6 $((Z)_2,+,\cdot)$ 是 2 阶整数方阵环，设

$$A=\begin{bmatrix}0&1\\0&0\end{bmatrix}\qquad B=\begin{bmatrix}1&0\\0&0\end{bmatrix}$$

则 $AB=0$，因此 A,B 分别是 $(Z)_2$ 的左、右零因子。

例 9.1.7 $(Z_6,+,\cdot)$ 中，$\bar{2}\cdot\bar{3}=\bar{0}$，因此 $\bar{2}$ 和 $\bar{3}$ 分别是 Z_6 的左、右零因子。

可见如果环中存在左(右)零因子，则乘法消去律不成立。

定理 9.1.1 环 R 中乘法消去律成立的充要条件是 R 中没有左(右)零因子。

证明：设 R 中没有左零因子，因而也就没有右零因子。以下只讨论没有左零因子的情况。充分性，设 $a\neq0$，$ab=ac$，则 $ab+(-ac)=ab-ac=a(b-c)=0=a0$，故 $b-c=0$，即 $b=c$；同理当 $ba=ca$ 时，$ba+(-ca)=ba-ca=(b-c)a=0=0a$，故 $b=c$，所以 R 中乘法消去律成立。必要性，对任意 $a,b\in R$，若 $ba=0$ 且 $a\neq0$，则由 $ba=0=0a$ 和消去律得到 $b=0$，因此 R 中任意非零元 a 不存在左零因子 b，使 $ba=0$。

当对环 R 增加若干限制后，可以得到不同类型的环。

定义 9.1.3 设 R 是环，$(R,\cdot)$ 是 R 的乘法半群。

1. 若 $(R,\cdot)$ 中有单位元 1，称 R 是有单位环。
2. 若 $(R,\cdot)$ 是交换半群，称 R 是交换环。
3. 若 $(R,\cdot)$ 是交换环，且没有零因子，称 R 是一个整环。
4. 若 $(R,\cdot)$ 中至少有两个元素，用 R^* 表示 R 中一切非零元的集合，如果 $(R^*,\cdot)$ 是群，则称 R 是一个除环。

例如整数环 $(Z,+,\cdot)$ 是有单位环，1 是其单位元；由于乘法适合交换律，所以它也是交换环，Z 中没有零因子，所以也是整环。但由于 $(Z^*,\cdot)$ 中只有 1 和 -1 有逆元，即它不是群，故 Z 不是除环。但是数环 Q，R 和 C 都是整环，同时也是除环。

例 9.1.8 设 $S=\{a,b\}$，则 $(S,+,\cdot)$ 是一个整环，其中运算 $+$，$\cdot$ 定义如下：

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	a	a
b	a	b

因为易见 $(S,+)$ 是加法群，a 是零元，$(S,\cdot)$ 是半群，有单位元 b，且运算 $\cdot$ 适合交换律，也没有零因子，所以 S 是整环，同时也可以得出 S 是除环。

从定义看，除环 R 中一定有单位元 1，因为 R^* 是 R 的子群，所以 R^* 中有单位元，它对任意 $a\in R^*$，满足 $a\cdot 1=1\cdot a=a$；对 R 中的零元，也有 $0\cdot 1=1\cdot 0=0$，因此 $(R,\cdot)$ 是幺群。但由于 $(R^*,\cdot)$ 是群，即对任意 $a,b\in R^*$，都有 $ab\in R^*$，不过 $0\notin R^*$，所以 $ab\neq 0$，因此除环中没有零因子，即除环中乘法消去律成立。

比如例 9.1.4 中的环 $(S,+,\cdot)$ 也是一个除环。因为 $(S,\cdot)$ 中有单位元 b，对任意 $x\in S$，都有 $xb=bx=x$，且 $(R,\cdot)$ 满足交换律，除了零因子 a 以外，b,c 之间的乘积都不等于 a，因此 S 是整环，同样易证 $S^*=S-\{a\}$ 是群，故它是个除环。

例 9.1.9 形如 $a+bi+cj+dk$ 的一个数称为四元数，其中 i,j,k 为符号，a,b,c,d 是实系数。规定两个四元数的加法运算是将它们的系数分别相加减，即

$$
\begin{aligned}
&(a_1+b_1i+c_1j+d_1k)+(a_2+b_2i+c_2j+d_2k)\\
&=(a_1+a_2)+(b_1+b_2)i+(c_1+c_2)j+(d_1+d_2)k。
\end{aligned}
$$

规定符号 i,j,k 的乘法表如下：

$\cdot$	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

这样，两个元素相乘按分配律展开后并项，例如

$$
\begin{aligned}
&(a_1+b_1i+c_1j+d_1k)(a_2+b_2i+c_2j+d_2k)\\
&=a_1a_2+a_1b_2i+a_1c_2j+a_1d_2k+b_1a_2i+b_1b_2i^2+b_1c_2ij+b_1d_2ik\\
&\quad+c_1a_2j+c_1b_2ji+c_1c_2j^2+c_1d_2jk+d_1a_2k+d_1b_2ki+d_1c_2kj+d_1d_2k^2\\
&=(a_1a_2-b_1b_2-c_1c_2-d_1d_2)+(a_1b_2+b_1a_2)+(c_1d_2-d_1c_2)i
\end{aligned}
$$

$$+(a_1c_2-b_1d_2+c_1a_2+d_1b_2)j+(a_1d_2+b_1c_2-c_1b_2+d_1a_2)k。$$

这样，全体四元数的集合 R 关于加法和乘法运算构成除环。因为是交换半群且有零元 $0=0+0i+0j+0k$，每个元 $a+bi+cj+dk$ 都有负元 $-a-bi-cj-dk$，故 $(R,+)$ 是交换群。$(R,\cdot)$ 中乘法运算适合结合律，并对加法满足分配律，故 $(R,+,\cdot)$ 是环。另外对 $(R^*,\cdot)$ 来说，对任意 $u=a+bi+cj+dk\neq0$，$(a+bi+cj+dk)(1+0i+0j+0k)=a+bi+cj+dk$，所以 $1+0i+0j+0k$ 是单位元，而且对每个 u，都有其共轭四元数 $\bar{u}=a-bi-cj-dk$，保证 u 在 R^* 中存在逆元

$$u^{-1}=\frac{1}{u\bar{u}}\bar{u},$$

其中

$$u\bar{u}=a^2+b^2+c^2+d^2。$$

于是 $(R^*,\cdot)$ 成群。故 $(R,+,\cdot)$ 是一个除环，称之为四元群除环。

如果一个除环是可交换的，那么称它是一个域。关于域我们在 9.4 节中再进行介绍。

定义 9.1.4 设 $(R,+,\cdot)$ 是一个环，S 是 R 的一个非空子集，如果 $(S,+,\cdot)$ 也是一个环，则称 S 是 R 的一个子环，也称 R 是 S 的一个扩环。易见，如果 S 是 R 的一个子环，则 $(S,+)$ 是 $(R,+)$ 的子群，同时 $(S,\cdot)$ 是 $(R,\cdot)$ 的子半群，并且在 S 中运算 $\cdot$ 对 $+$ 适合分配律。

例 9.1.10 设 Z 是整数环，令 $S=nZ$，n 是正整数，则 S 是 Z 的子环。因为易证 $(S,+)$ 是子群，$(S,\cdot)$ 是子半群，且对任意 $na,nb,nc\in nZ$，

$$\begin{aligned}na(nb+nc)&=(na)(n(b+c))=n^2(a(b+c))\\&=n^2(ab+ac)=n^2(ab)+n^2(ac)\\&=(na)(nb)+(na)(nc)。\end{aligned}$$

同理

$$(nb+nc)na=(nb)(na)+(nc)(na)。$$

因此 S 是整数环 Z 的子环。

定理 9.1.2 设 S 是 R 的子集，它是 R 的子环的充要条件是对任意的 $a,b\in S$，都有 $a-b,ab\in S$。

证明：只证其必要性，因为 S 是 R 的子环，故 $(S,+)$ 是群，因此对任意 $a,b\in S$，$a+b\in S$，$-b\in S$，所以 $a+(-b)=a-b\in S$，又因 $(S,\cdot)$ 是半群，它对乘法封闭，所以 $ab\in S$。其充分性请读者自行证明。

使用这个定理可以比较方便地判断一个子环。比如对例 9.1.10 来说，因为 $na-nb=n(a-b)\in S$，$(na)(nb)=n(nab)\in S$，所以 S 是 Z 的子环。

例 9.1.11 设 S_1、S_2 都是 R 的子环，则 $S_1\cap S_2$ 也是 R 的子环。

证明：因为 $0\in S_1\cap S_2$，所以 $S_1\cap S_2$ 非空，对任意 $a,b\in S_1\cap S_2$，由于 S_1、S_2 都是子环，由定理 9.1.2，$a-b\in S_1$，$a-b\in S_2$，$ab\in S_1$，$ab\in S_2$，亦即 $a-b\in S_1\cap S_2$，$ab\in S_1\cap S_2$。因此 $S_1\cap S_2$ 是 R 的子环。

同理可以推出，如果 S_i 是 R 的子环，$i=1,2,\cdots,t$，则 $\bigcap_{i=1}^{t}S_i$ 也是 R 的子环。而且如果 A 是 R 的一个非空集合，则 R 中总有包含 A 的子环。所有这些子环的交集显然也是含有 A 的最小子环，这个子环也称为由 A 生成的子环。

当 R 分别是整环、除环时，相应地也有子整环、子除环的概念。

9.2 理想、商环

定义 9.2.1 设 R 是一个环，$(D,+)$是$(R,+)$的一个子加法群。

1. 若对任意的 $a\in R$，都有

$$aD=\{ad\mid d\in D\}\subseteq D\ ,$$

则称 D 是 R 的一个左理想。

2. 若 a 满足

$$Da=\{da\mid d\in D\}\subseteq D\ ,$$

称 D 是 R 的一个右理想。

3. 若 D 既是 R 的左理想，又是右理想，则称 D 是 R 的一个理想。

如果 $D=R$ 或 $D=\{0\}$，则 D 也是 R 的理想，并称它们是平凡理想。如果 $D\subset R$，称它是 R 的真理想。如果 R 除平凡理想外没有别的理想，则称 R 是单环。因此如果$(R,+)$是单群，则 R 一定是单环。

例 9.2.1 n 阶实矩阵的集合$(R)_n$关于矩阵的加法和乘法构成环，称之为矩阵环。设 D 是$(R)_n$中一切形如

$$\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1(n-1)} & 0 \\ x_{21} & x_{22} & \cdots & x_{2(n-1)} & 0 \\ \cdots\cdots & & & & \\ x_{n1} & x_{n2} & \cdots & x_{n(n-1)} & 0 \end{bmatrix} \qquad x_{ij}\in R$$

的矩阵构成的集合，易证 D 是$(R)_n$的一个子加群，而且对任意 $A\in(R)_n$，$B\in D$，都有 $AB\in D$，即 D 是$(R)_n$的一个左理想，反之如果 D'是$(R)_n$中一切形如

$$\begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1n} \\ y_{21} & y_{22} & \cdots & y_{2n} \\ \cdots\cdots & & & \\ y_{(n-1)1} & y_{(n-1)2} & \cdots & y_{(n-1)n} \\ 0 & 0 & \cdots & 0 \end{bmatrix} \qquad x_{ij}\in R$$

的矩阵构成的集合，则 D'是$(R)_n$的一个右理想。

例 9.2.2 设 $D_m=\{mk\mid k\in Z\}$，则 D_m 是整数环 Z 的一个理想，其中 m 是正整数。

证明：显然 D_m 是 Z 的一个子加群，对任意 $a\in Z$，$aD_m=\{a(mk)\mid mk\in D_m\}\subseteq\{m(ak)\mid ak\in Z\}=D_m$，同时 $D_ma=\{(mk)a\mid mk\in D_m\}\subseteq\{m(ak)\mid ak\in Z\}=D_m$，因此 D_m 是 Z 的一个理想。

根据理想的定义，可以与定理 9.1.2 相类似地得到如下定理：

定理 9.2.1 设 D 是 R 的非空子集，D 是 R 的理想的充要条件是：

1. 对任意 $a,a'\in D$，都有 $a-a'\in D$。

2. 对任意 $a\in D$，$b\in R$，都有 $ab\in D$，$ba\in D$。

利用该定理能够比较容易地判定 R 的理想。比如用它容易证明例 9.2.2 中的 D_m 是 Z 的一个理想。而例 9.2.1 中的 D 不是 R 的理想，因为如果设 D 是 R 的左理想，则由于

存在 $B=(b_{ij})_{n\times n}\in R$，其中 $b_{ij}\neq 0$，使得 $DB\not\subseteq D$，因此 D 并不同时是右理想，从而说明 D 不是 R 的理想。

从理想的定义也可以得到，R 中若干理想的交集仍然是一个理想；若 S 是 R 的一个子集，则 R 中全部包含 S 的理想的交集 (S) 也是包含 S 的一个理想，我们称 (S) 是由 S 生成的理想。下面分析一下 (S) 中的元素情况。如果 S 是有限集，设 $S=\{a_1,a_2,\cdots,a_n\}$，可以用 $(a_1,a_2,\cdots,a_n)$ 表示理想 (S)。设 $x,x',y,y'\in R$，一定有 $xa_i\in(S)$，$a_iy\in(S)$，故 $xa_iy=xa_k\in(S)$，但是由于 $xa_iy+x'a_iy'$ 无法合并，因此理想 $(a_1,a_2,\cdots,a_n)$ 的元素应是全部形如

$$\sum_{i_1} x_{1i_1}a_1y_{1i_1}+\sum_{i_2} x_{2i_2}a_2y_{2i_2}+\cdots+\sum_{i_n} x_{ni_n}a_ny_{ni_n}$$

的元素。

若 R 是可交换环，则由于 $xax'=x''a$，$x''\in R$，因此理想 $(a_1,a_2,\cdots,a_n)$ 中的元素可以简化为形如 $\sum_{i=1}^{n} x_i a_i$，其中 $x_i\in R$，特别当 (S) 是仅由元素 a 生成的理想 (a) 时，它的元素是 xa，$x\in R$，即

$$(a)=\{xa\,|\,x\in R\}=R_a,$$

并称之为由 a 生成的主理想，当然 $Ra=aR$。

比如在例 9.2.2 中，因为 $D_m=\{mk\,|\,k\in Z\}$，所以 D_m 是由 m 生成的主理想，记作 (m)。事实上，整数环 Z 的每一个理想都是主理想。

理想在环的理论中所起的作用类似于正规子群在群论中的作用。

设 D 是环 R 的一个理想，由于 $(R,+)$ 是交换群，$(D,+)$ 是 $(R,+)$ 的子群，故 $(D,+)$ 是正规子群，因此可以得到 $(R,+)$ 对于 $(D,+)$ 的商群 R/D。

上述的商群 R/D 关于环 R 的二元运算也可以作成环。下面我们来构造这个环。

对任意 $a\in R$，a 所在的剩余类

$$\bar{a}=\{a+x\,|\,x\in D\}=a+D\,,$$

或者

$$R/D=\{a+D\,|\,a\in R\}=\{\bar{a}\,|\,a\in R\}。$$

这样，对任意 $\bar{a},\bar{b}\in R/D$，有 $\bar{a}+\bar{b}=\overline{a+b}$，显见 $(R/D,+)$ 是交换群。在 R/D 中用 R 的乘法来规定

$$\bar{a}\cdot\bar{b}=\overline{a\cdot b},\ a,b\in R\ 。$$

我们证明 $(R/D,\cdot)$ 是半群，首先 $\cdot$ 是 R/D 上的一个二元运算，因为对任意 $\bar{a},\bar{b}\in R/D$，$\bar{a}\,\bar{b}=\overline{ab}\in R/D$，同时它与代表元的选择无关，亦即假定 $a_1\in\bar{a}$，$b_1\in\bar{b}$，应有 $\overline{a_1b_1}=\overline{ab}$。因为设 $a_1=a+x_1$，$b_1=b+x_2$，$x_1,x_2\in D$，则

$$\overline{a_1b_1}=\overline{(a+x_1)(b+x_2)}=\overline{a+b_1+ax_2+x_1b+x_1x_2}。$$

由于 D 是理想，所以

$$ax_2+x_1b+x_1x_2=d\in D\,,$$

亦即

$$\overline{a_1b_1}=\overline{a_1b_1}=\overline{ab+d}=\overline{ab}。$$

所以 $\cdot$ 也是 R/D 中的二元运算。对任意 $\bar{a}$，$\bar{b}$，$\bar{c}\in R/D$，

$$(\bar{a}\,\bar{b})\bar{c}=\bar{a}\,\bar{b}\,\bar{c}=\overline{(ab)c}=\overline{a(bc)}=\bar{a}\,\overline{bc}=\bar{a}(\bar{b}\,\bar{c})。$$

故 $(R/D,\cdot)$ 是一个半群。

再证 R/D 作成环，即乘法对加法适合分配律，由于

$$\bar{a}(\bar{b}+\bar{c})=\bar{a}(\overline{b+c})=\overline{a(b+c)}$$
$$=\overline{ab+ac}=\overline{ab}+\overline{ac}=\bar{a}\,\bar{b}+\bar{a}\,\bar{c}。$$
$$(\bar{b}+\bar{c})\bar{a}=\overline{b+ca}=\overline{(b+c)a}=\overline{ba+ca}$$
$$=\overline{ba}+\overline{ca}=\bar{b}\,\bar{a}+\bar{c}\,\bar{a}。$$

综上可知$(R/D,+,\cdot)$是一个环。这个环称为 R 关于理想 D 的商环。

定义 9.2.2 设 R 是一个环，D 是 R 的一个理想，则商群 R/D 关于乘法 $\bar{a}\,\bar{b}=\overline{ab}$所作成的环叫作 R 关于 D 的商环，记作 R/D。

例 9.2.3 $D_m=(4)$是整数环 Z 的一个理想，$Z/(4)$是一个商环，由于 $\bar{a}=a+(4)$，故它含 4 个元素：$\bar{0}$，$\bar{1}$，$\bar{2}$，$\bar{3}$。其加法表和乘法表如下：

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

可见 $Z/(4)=Z_4$，一般说来，有 $Z/(M)=Z_m$。

定义 9.2.3 设 D 是 R 的一个真理想，若 R 中不存在包含 D 的真理想，则称 D 是 R 的一个极大理想。

例 9.2.4 (p)是整数环的一个理想，其中 p 是素数，则(p)是极大理想，因为假定 H 是真包含(p)的 Z 的一个理想，则存在 $q\in H\setminus(p)$，由于$(q,p)=1$，因此 $a,b\in Z$ 使 $ap+bq=1\in H$，$\therefore H=z$，即(p)是极大理想。

定义 9.2.4 设 D 是可交换环 R 的一个理想，若对于任意的 $a,b\in R$，如果 $ab\in D$，就有 $a\in D$ 或 $b\in D$，则称 D 是 R 的一个素理想。

例 9.2.5 (p)是整数环 Z 的一个素理想，其中 p 是素数，因为若 $ab\in(p)$则一定有 $p|ab$，由于 p 是素数，故必有 $p|a$ 或 $p|b$，即 $a\in(p)$或 $b\in(p)$。

素理想和极大理想可以用来判断环和域。

9.3 环 的 同 态

定义 9.3.1 设 R 和 R'是环，f 是 R 到 R'的一个映射。如果对任意的 $a,b\in R$，都有

$$f(a+b)=f(a)+f(b)$$
$$f(ab)=f(a)f(b)$$

则称 f 是 R 到 R'的一个同态映射，或称为同态。当 f 分别是单射，满射和双射时，分别称为单一同态，满同态和同构。我们仍用 $R\sim R'$表示满同态，$R\cong R'$表示同构。

同构是单一同态，也是满同态。

例 9.3.1 已知$(Z,+,\cdot)$和$(Z_n,+,\cdot)$都是环。设 $f: a\to\bar{a}$，对任意 $a\in Z$，则 f 是 Z 到 Z_n 的满同态。

显然 f 是 Z 到 Z_n 的一个映射，而且对任意 $\bar{a}\in Z_n$，存在 $a\in Z$，满足 $f(a)=\bar{a}$，所以 f 是满射。又由于对任意 $a,b\in Z$，

$$f(a+b)=\overline{a+b}=\bar{a}+\bar{b}=f(a)+f(b)。$$

$$f(ab)=\overline{ab}=\bar{a}\,\bar{b}=f(a)f(b)。$$

即 f 是 Z 到 Z_n 的一个同态映射。故 $Z\sim Z_n$。

例 9.3.2 令

$$R=\left\{\begin{bmatrix}a & b\\0 & c\end{bmatrix}\,|a,\,b,\,c\in Z\right\}$$

$$R'=\left\{\begin{bmatrix}a & 0\\0 & c\end{bmatrix}\,|a,\,c\in Z\right\}$$

$(R,+,\cdot)$和$(R',+,\cdot)$都是环，设

$$f:\begin{bmatrix}a & b\\0 & c\end{bmatrix}\to\begin{bmatrix}a & 0\\0 & c\end{bmatrix}$$

则 $R\sim R'$。

证明：显然 f 是 R 到 R' 的满射，同时对任意 $A,B\in R$，设

$$A=\begin{bmatrix}a & b\\0 & c\end{bmatrix}\qquad B=\begin{bmatrix}\alpha & \beta\\0 & \gamma\end{bmatrix}$$

$$f(A+B)=f\begin{bmatrix}a+\alpha & b+\beta\\0 & c+\gamma\end{bmatrix}=\begin{bmatrix}a+\alpha & 0\\0 & c+\gamma\end{bmatrix}$$

$$=\begin{bmatrix}a & 0\\0 & c\end{bmatrix}+\begin{bmatrix}\alpha & 0\\0 & \gamma\end{bmatrix}=f(A)+f(B)。$$

$$f(AB)=f\begin{bmatrix}a\alpha & a\beta+b\gamma\\0 & c\gamma\end{bmatrix}=\begin{bmatrix}a\alpha & 0\\0 & c\gamma\end{bmatrix}$$

$$=\begin{bmatrix}a & 0\\0 & c\end{bmatrix}\begin{bmatrix}\alpha & 0\\0 & \gamma\end{bmatrix}=f(A)f(B)。$$

故 $R\sim R'$。

例 9.3.3 设 D 是环 R 的一个理想，对任意 $a\in R$，令 $f:a\to\bar{a}$，$\bar{a}$ 是商环 R/D 中 a 所在的剩余类，则 f 是 R 到 R/D 的一个满同态，这个同态称为环 R 到其商环 R/D 的自然同态，R/D 是 R 的同态象。

诸如群的同态，关于环的同态有以下结论。

设 R 是一个环，S 是有加法和乘法运算的代数系统。如果 f 是 R 到 S 的一个同态，则 R 的象 $R'=f(R)\subseteq S$ 也是一个环。$f(0)$是 R' 中的零元 $0'$，$f(-a)=-f(a)$。如果 R 中有单位元 1 而 R' 中不只有一个元素，则 R' 中也有单位元 $1'$，而且 $f(1)=1'$；若 $a\in R$ 有逆元 a^{-1}，则 $f(a^{-1})=(f(a))^{-1}\in R'$。

定理 9.3.1 设 R 和 R' 都是环，其零元分别是 0 和 $0'$，f 是 R 到 R' 的同态，则 $K=\{x\in R\,|\,f(x)=0'\}$是 R 的理想，并称之为同态 f 的核，记作 $K=\mathrm{Ker}f$。

证明：由于 f 是同态，根据定义 f 也是群$(R,+)$到$(R',+)$的同态，所以 K 是群同态的核，故$(K,+)$是$(R,+)$的子群。对任意 $a\in R,k\in K$，由于

$$f(ka)=f(k)f(a)=0'f(a)=0'。$$
$$f(ak)=f(a)f(k)=f(a)\cdot 0'=0'。$$
所以 $ka,ak\in K$，因此 $K=\mathrm{Ker}f$ 是 R 的一个理想。

因为同态核 K 是 R 的一个理想，这样设 a' 是 R' 的任意元，则 a' 的原象 $f^{-1}(a')=\{a\in R\mid f(a)=a'\}$ 一定是 K 的一个剩余类。同时利用同态核也可以判断一个同态是否为单一同态。

定理 9.3.2 设 f 是 R 到 R' 的一个同态映射，则 f 是单一同态的充要条件是 $\mathrm{Ker}f=\{0\}$。

证明：必要性。设 f 是单一同态，则 f 是 R 到 R' 的一个单射，所以对 R' 中的零元 $0'$，在 R 中只有一个原象 0，满足 $f(0)=0'$，故 $\mathrm{Ker}f=\{0\}$。充分性。若 $\mathrm{Ker}f=\{0\}$，对任意 $a,b\in R$，且 $f(a)=f(b)$，则 $f(a)-f(b)=0'$，即 $f(a-b)=0'$，故 $a-b=0$，亦即 $a=b$，所以 f 是单射，因此 f 是 R 到 R' 的一个单一同态。

同态核 $\mathrm{Ker}f$ 是环 R 的一个理想，那么如果给定 R 的任意一个理想 D，是否存在一个环 R'，能够使 R 到 R' 之间存在一个同态 f，而且使 $\mathrm{Ker}f=D$ 呢？

由于 D 是 R 的一个理想，所以 R/D 是 R 的一个商环，如果在 R 与 R' 之间建立一个关系

$$f(a)=\bar{a}=a+D\text{，}\quad 对任意 a\in R。$$

则 a 对应唯一确定的剩余类 $\bar{a}=a+D\in R/D$，这样规定的 f 便是加法群 $(R,+)$ 到 $(R/D,+)$ 的一个满同态映射，我们再规定 $\bar{a}\,\bar{b}=\overline{ab}$ 的乘法运算，于是对任意 $a,b\in R$ $f(ab)=\overline{ab}=\bar{a}\,\bar{b}=f(a)f(b)$，所以 f 是环 R 到环 $R'=R/D$ 的一个同态映射。

因此可以得到：按照剩余类的加法和乘法运算，R 关于理想 D 的所有剩余类的集合 R/D 也是一个环（即商环），若规定 $f:a\to a+D$，则 f 是 R 到 R/D 的一个满同态，而且 $\mathrm{Ker}f=D$。

下面介绍同态基本定理。

同态基本定理：设 R 是一个环，则 R 的任一商环都是 R 的同态象，而且若 R' 是 R 在 f 作用下的同态象，则 $R'\cong R/\mathrm{Ker}f$。

定理的前半部分在上面已经证明，因为对任一商环 R/D，$f:a\to a+D$ 是满同态，故 $R\sim R/D$。下面我们证明后半部分。因为 $R'=f(R)$，$\mathrm{Ker}f=D$ 是 R 的一个理想，所以有商环 R/D。在商环 R/D 和 R' 之间建立关系：

$$\varphi:\bar{a}\to f(a)\text{，}\quad 对任意 \bar{a}\in R/D。$$

我们证明 φ 是 R/D 到 R' 的同构。

对任意 $\bar{a}\in R/D$，有 $\varphi(\bar{a})=f(a)\in R'$，另外若 $\overline{a_1}=\bar{a}$，则 $a_1=a+x$，$x\in\mathrm{Ker}f$。于是

$$\begin{aligned}\varphi(\overline{a_1})&=\varphi(\overline{a+x})=f(a+x)=f(a)+f(x)\\&=f(a)+0'=f(a)。\end{aligned}$$

其中 $0'$ 是 R' 中的单位元。因此 φ 是 R/D 到 R' 的一个映射，显然它也是满射。同时对任意 $a,b\in R/D$，有

$$\begin{aligned}\varphi(\bar{a}+\bar{b})&=\varphi(\overline{a+b})=f(a+b)=f(a)+f(b)\\&=\varphi(\bar{a})+\varphi(\bar{b})。\end{aligned}$$

$$\varphi(\bar{a}\,\bar{b}) = \varphi(\overline{ab}) = f(ab) = f(a)f(b) = \varphi(\bar{a})\varphi(\bar{b})。$$

因此 φ 是满同态。再者，对任意元素 $\bar{a}\in R/D$，若 $\bar{a}\in \mathrm{Ker}\varphi$，则 $\varphi(\bar{a})=0'=f(a)$，故 $a\in \mathrm{Ker}f$，于是得到 $\bar{a}=\mathrm{Ker}f$。亦即 $\mathrm{Ker}f=\{\bar{a}\,|\,\bar{a}=\mathrm{Ker}f\}=\{D\}$，由定理 9.3.2 得知 φ 是单射，因此 φ 是同构，即 $R'\cong R/\mathrm{Ker}f$。

根据同态基本定理，我们可以得到

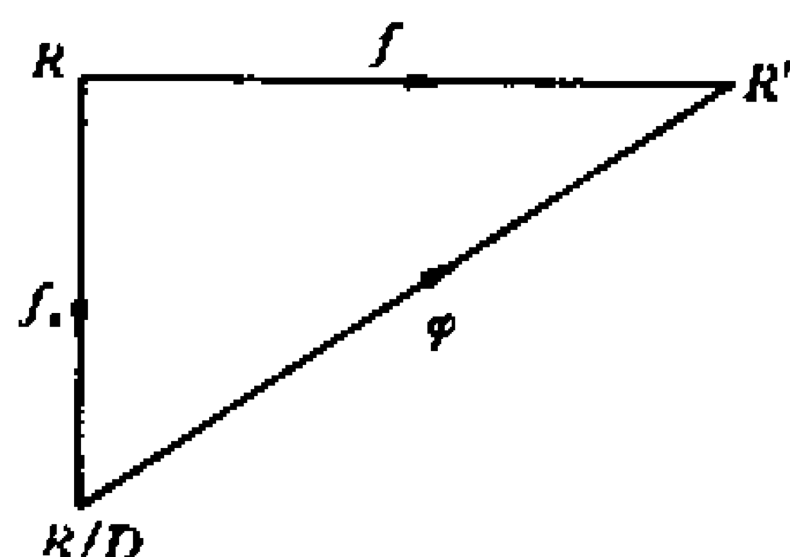


图 9.1

推论：设 f 是 R 到 R' 的满同态，D 是 R 的一个理想，$f_\cdot$ 是 R 到其商环 $R/\mathrm{Ker}f$ 的自然同态，则一定存在 R/D 到 R' 的满同态 φ，使

$$f = \varphi f_\cdot。$$

其图形表示如图 9.1。

例 9.3.4 设 R 是环，A、B 是 R 的两个理想，且 $B\subseteq A$，则 A/B 是 R/B 的理想，同时

$$\frac{R/B}{A/B}\cong R/A。$$

证明：因为 A、B 是 R 的理想，故 R/A，R/B 都是环。下面需要证明 A/B 是 R/B 的理想，且存在图 9.2 中的同构 φ。

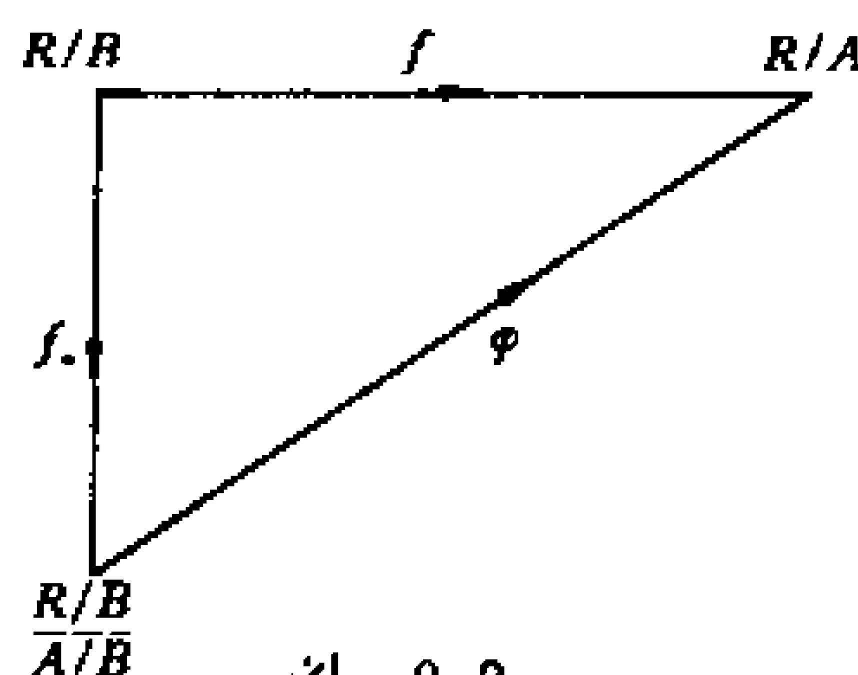


图 9.2

由同态基本定理，如果 f 是 R/B 到 R/A 的满射，且 $\mathrm{Ker}f=A/B$，则问题得证。设对任意 $a\in R$，$f: a+B\to a+A$，于是对任意 $a,b\in R$，若 $a+B=b+B$，则 $a-b\in B$，亦即 $a-b\in A$，故 $a+A=b+A$，所以 f 是 R/B 到 R/A 的映射，同时对任意的 $a+A\in R/A$，都存在 $a+B\in R/B$，使 $f(a+B)=a+A$，故 f 是满射，而且

$$\begin{aligned} f((a+B)+(b+B)) &= f((a+b)+B) = (a+b)+A \\ &= (a+A)+(b+A) = f(a+B)+f(b+B)。\\ f((a+B)(b+B)) &= f(ab+B) = ab+A \\ &= (a+A)(b+A) = f(a+B)f(b+B)。\end{aligned}$$

所以 f 是 R/B 到 R/A 的满同态，另一方面，$\mathrm{Ker}f=\{x+B\,|\,x+A=A\}$，但 $x+A=A$ 即是 $x\in A$，因此

$$\mathrm{Ker}f = \{x+B\,|\,x\in A\} = A/B。$$

故定理得证。

下面给出另一个重要的环的同构定理。

定理 9.3.3 令 R 是环，S 是子环，D 是 R 的一个理想，则 $S+D=\{s+d\,|\,s\in S,d\in D\}$ 是以 D 作为一个理想的 R 的子环，$S\cap D$ 是 S 的理想，而且存在 $(S+D)/D$ 到 $S/(S\cap D)$ 的一个同构

$$\varphi: s+D\to s+(S\cap D),\ s\in S。$$

证明：D 是 R 的理想，当然也是 R 的子环。设 $s+d$，$s'+d'\in S+D$，由于

$$(s+d)-(s'+d')=(s-s')+(d-d')\in S+D。$$
$$(s+d)(s'+d')=ss'+ds'+(s+d)d'。$$
其中 $ss'\in S$，$ds'+(s+d)d'\in D$，因此 $(s+d)(s'+d')\in S+D$，由定理 9.1.2，$S+D$ 是 R 的一个子环，同时显然 D 是 $S+D$ 的一个理想，故商环 $(S+D)/D$ 有意义。由于 R 到 R/D 存在自然同态 f^*，而 S 是 R 的子环，如果把自然同态 f^* 的原象严格控制在 S 中，那么对任意 $s\in S$，$f: s\to s+D$ 也是一个同态，它的象很清楚是 $(S+D)/D$。该同态的核是满足 $s+D=D$ 的全部 s 的集合，这就是 $S\cap D$。于是可以得到图 9.3。

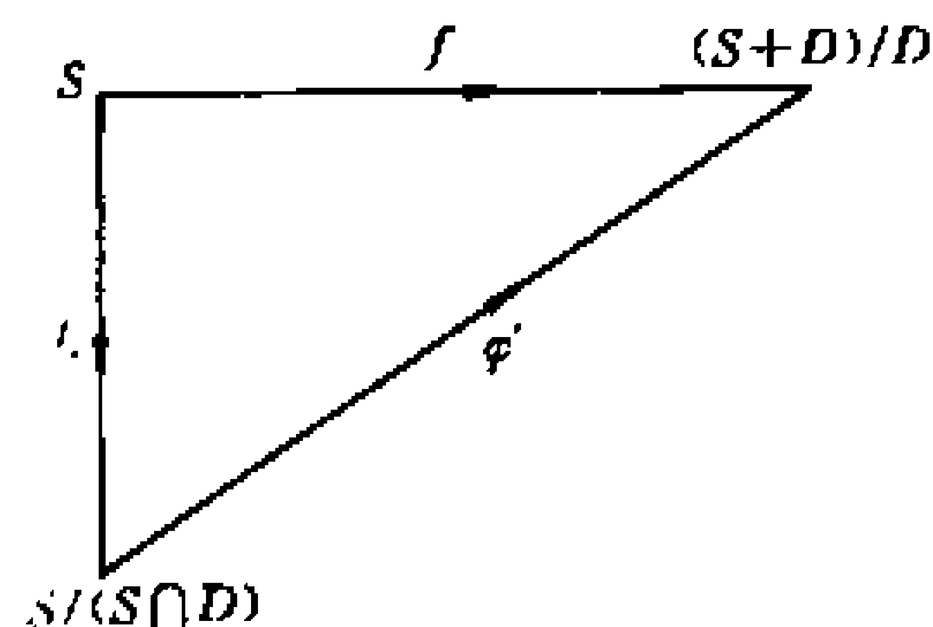


图 9.3

由同态基本定理，$\varphi': s+(S\cap D)\to s+D$ 是 $S/(S\cap D)$ 到 $(S+D)/D$ 的一个同构，它的逆映射 φ 就是所求的同构。

依据同态基本定理，也可以证明以下一些结论。

定理 9.3.4 设环 R 与 R' 同态，则 R 与 $\mathrm{Ker}f$ 之间的子环与 R' 的子环之间一一对应。

定理 9.3.5 设 D 是 R 的真理想，则 D 是 R 的极大理想的充要条件是 R/D 是单纯环。

定理的证明留作练习。

9.4 域的概念

在 9.1 节中我们曾给出除环的定义，即如果环 R 中至少有两个元素，令 R^* 表示 R 中一切非零元的集合，若 $(R^*,\cdot)$ 是群，则称 R 是一个除环。如果对除环再增加一点限制，又可以得到称为域的另一代数系统。

定义 9.4.1 若一个除环 R 是可交换的，就称它是一个域，记作 F。

根据定义，若 R 是域，则 $(R^*,\cdot)$ 一定是交换群，亦即

1. $(R^*,\cdot)$ 中有单位元，对所有 $a\in R$，
$$1\cdot a=a\cdot 1=a。$$

2. 对 R 中每个非零元 a，都存在其逆元 a^{-1}，满足
$$aa^{-1}=a^{-1}a=1。$$

由于域 F 也是除环，所以域中至少存在两个元素。

例 9.4.1 $(R,+,\cdot)$，$(Q,+,\cdot)$ 和 $(C,+,\cdot)$ 都是域，而 $(Z,+,\cdot)$ 不是域，因为 $(Z^*,\cdot)$ 不是群。

例 9.4.2 $(Z_3,+,\cdot)$ 的运算表如下：

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

显见它是一个除环，同时(Z_3^*，+，·)适合交换律，故(Z_3，+，·)是一个域。

例 9.4.3 一个有单位元 1 的有限整环是一个域。

证明：设 R 是一个有单位元 1 的有限整环，因此(R，·)是交换半群，且没有零因子，由 R^* 是非空集合，可知(R^*，·)是有单位元 1 的半群。下面只要证明在(R^*，·)中任意元 a 都有逆元 a^{-1}。依据定理 9.1.1，R 中乘法消去律成立，这样对于 $x_i, x_j \in R$ 且 $x_i \neq x_j$，有 $ax_i, ax_j \in R$ 且 $ax_i \neq ax_j$。因为 R 是有限集，所以一定存在且只存在一个 $x_k \in R$，满足 $ax_k = 1$，即 $x_k = a^{-1}$，因此 R 是一个域。

定理 9.4.1 设 F 是一个域，则对于任意的 $a, b \in R$，$b \neq 0$，方程 $bx = a$ 在 F 中有唯一解。

证明：因为 F 是域，所以 F 中没有零因子，且由于 $b \neq 0$，故 b 有逆元 b^{-1}，因此从 $bx = a$ 可导出 $b^{-1}bx = b^{-1}a$，亦即 $x = b^{-1}a$，x 有唯一解。

因为 x 是唯一的，所以 $b^{-1}a$ 也可以写成商的形式：$\frac{a}{b}$，在域中，商具有下述性质：

(1) 设 $b, d \neq 0$，当且仅当 $ad = bc$ 时，$\frac{a}{b} = \frac{c}{d}$。证明：由 $ad = bc$，且 b、$d \neq 0$，因为消去律成立，将两端同乘 $b^{-1}d^{-1}$，有 $b^{-1}a = d^{-1}c$，即 $\frac{a}{b} = \frac{c}{d}$。反之，设 $\frac{a}{b} = \frac{c}{d}$，两端同乘以 bd，则有 $ad = bc$。

(2) 设 b、$d \neq 0$，则 $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$。

证明：
$$\begin{aligned}\frac{a}{b} \pm \frac{c}{d} &= b^{-1}a \pm d^{-1}c = b^{-1}d^{-1}da \pm d^{-1}b^{-1}bc \\ &= (d^{-1}b^{-1})(ad) \pm (d^{-1}b^{-1})(bc) \\ &= (bd)^{-1}ad \pm (bd)^{-1}bc \\ &= (bd)^{-1}(ad \pm bc) \\ &= \frac{ad \pm bc}{bd}\,。\end{aligned}$$

(3) 设 b、$d \neq 0$，则 $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$。

因为
$$\frac{a}{b} \cdot \frac{c}{d} = (b^{-1}a)(d^{-1}c) = b^{-1}(ad^{-1})c$$
$$= b^{-1}d^{1}ac = (db)^{-1}ac = (bd)^{-1}ac = \frac{ac}{bd}\,。$$

(4) 设 b、c、$d \neq 0$，则 $\frac{a}{b} \Big/ \frac{c}{d} = \frac{ad}{bc}$。

因为
$$\frac{a}{b} \Big/ \frac{c}{d} = b^{-1}a/d^{-1}c = (d^{-1}c)^{-1}(b^{-1}a)$$
$$= (c^{-1}d)(b^{-1}a) = (c^{-1}b^{-1})(da) = (bc)^{-1}(ad) = \frac{ad}{bc}\,。$$

观察环和域之间的关系，我们也有如下定理：

定理 9.4.2 F 是域的充要条件为：F 是有 1 元的交换的单纯环。

证明：充分性。只要证明 F 中每个非零元都有逆，因为 F 是单纯环，它只有两个理想，$\{0\}$，F。令 $a\in F$，$a\neq 0$，则由 a 生成的主理想 $(a)=aF$。又因 $a\neq 0$ 且 $a\in aF$，所以 $aF\neq\{0\}$，这样 $aF=F$。由于 F 中有 1 元，故 F 中一定存在一个元素 b，使 $ab=1$，则 b 是 a 在 F 中的逆元，故 F 是域。以下再证必要性。取 F 的任意理想 $D\neq\{0\}$，一定存在非零元 $a\in D$，由于 F 是域，故 $a^{-1}\in F$，因此 $a^{-1}D\subseteq D$，故 $a^{-1}a\in D$，亦即 $1\in D$。因此对任意 $x\in F$，$x1\in D$，即 $x\in D$，故 $F\subseteq D$，但 D 是 F 的理想，又有 $D\subseteq F$，所以 $D=F$，即 F 是单纯环，当然它也一定是可交换的，且有 1 元。

定义 9.4.2 设 $(F,+,\cdot)$ 是一个域，S 是 F 的一个非空子集。如果 S 关于 F 的运算 $+$，$\cdot$ 也构成域，则称 S 是 F 的一个子域。

在环 R 中我们知道，如果 S_i 是 R 的子环，$i=1,2,\cdots,t$，则它们的交集 $\bigcap_{i=1}^{t} S_i$ 也是 R 的子环。这个结论同样适合于域，即 F 中子域的交集仍是子域。设 A 是 F 的一个非空子集，则 F 中所有包含 A 的子域的交集是包含 A 的最小子域，称为由 A 生成的子域。

关于域还有许多重要的概念与定理，特别是有限域，在编码理论中有很重要的应用，这里就不再介绍了。

习 题 九

1. 证明环的性质 13 和 14。

2. 设 R 是有且仅有一个左单位元的环，证明 R 有单位元。

3. 证明在环 R 中，若元素 a 有左逆元 a' 和右逆元 a''，则一定有 $a'=a''$，且 a' 是 a 的唯一逆元。

4. 设 R 是除环，证明对任意 $a,b\in R$，$a\neq 0$，方程 $ax=b$ 在 R 中有解且仅有一个解。

5. 证明如果环 R 的加法群 $(R,+)$ 是循环群，则 R 是交换环。

6. 完成定理 9.1.2 的充分性证明。

7. 设 $(A,+,\cdot)$ 是一个环，对 A^A 规定加法与乘法：任取 $f,g\in A^A$，对任意 $x\in A$，令

$$(f+g)(x)=f(x)+g(x),$$
$$(f\cdot g)(x)=f(x)\cdot g(x)。$$

证明 $(A^A,+,\cdot)$ 是一个环。

再令 S 是 A 的一个子环，证明

$$R_s=\{f\in A^A \mid f(S)\subseteq S\}$$

是 $(A^A,+,\cdot)$ 的一个子环。

8. 设 $A_1,A_2,\cdots,A_n$ 都是环 R 的理想，证明

(1) $A_1+A_2+\cdots+A_n=\{a_1+a_2+\cdots+a_n \mid a_i\in A_i\}$，

(2) $A_1A_2\cdots A_n=\{a_1a_2\cdots a_n \mid a_i\in A_i\}$，

都是 R 的理想。

9. 设 R 是环，$a\in R$，令 $R_a=\{ra \mid r\in R\}$，证明 R_a 是 R 的一个左理想。

10. 设 R 是形如

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$$

整数二阶方阵环，令

$$D = \left\{ \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} \middle| x \in Z \right\}$$

证明 D 是 R 的理想。

11. 找出 Z_6 的所有理想。

12. 设 f 是 R 到 R' 的同态，D 是 D' 的理想，证明 $f^{-1}(D)$ 是 R 的理想。

13. 设 R，R' 是环，其中

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \middle| a, b, c \in Z \right\}$$

$$R' = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & x \end{bmatrix} \middle| x \in Z \right\}$$

证明：R' 是 R 的子环，找出 R 到 R' 的一个满同态 f，并求出 $\mathrm{Ker} f$。

14. 设 $R = Z \times Z$ 是关于以下定义的加法、乘法作成的环：

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2),$$

令 $f: (a, b) \rightarrow a$，对任意 $(a, b) \in R$，证明 f 是 R 到 Z 的一个同态。

15. 证明定理 9.3.4。

16. 证明定理 9.3.5。

17. 设 a，b 是有单位元环 R 上的二个可逆元，证明 ab 也是可逆元，且 $(ab)^{-1} = b^{-1}a^{-1}$。

18. 设 R 是有单位元的环，证明 R 中的可逆元一定不是零因子。

19. 设 R 是一个域，R' 是 R 的一个子环，证明 R' 是整环。

20. 构造一个含有两个元素的域，并说明之。

21. 给定代数系统 $(R, +, \cdot)$，其运算表如下：

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

证明：

(1) R 是一个域。

(2) 求解 R 中的方程组

$$\begin{cases} x + cy = a \\ cx + y = b \end{cases}$$

22. 设 R_1,R_2 是环,$R_1\times R_2$ 是环 R_1、R_2 的直积,其中加法乘法运算分别与题 14 相同,证明:

(1) $R_1\times R_2$仍然是一个环。

(2) 当 R_1、R_2 分别是有单位元环时,$R_1\times R_2$ 也是有单位环。

23. 设 S 是域 F 的一个子环,证明 S 是子域的充要条件是:对任意的 $x\in S$,$x\neq 0$,都有 $x^{-1}\in S$。

第十章　格与布尔代数

10.1　格及其基本性质

在集合论中，对集合中的元素可加入序的概念，从而有下面偏序集的定义

定义 10.1.1　对于一个集合 P 及 P 上一个二元关系 $\leqslant$，若对任意 a，b，$c \in P$，都满足：

(1) 自反性

(P-1)　　$a \leqslant a$。

(2) 反对称性

(P-2)　　$a \leqslant b$，$b \leqslant a \Rightarrow a=b$。

(3) 传递性

(P-3)　　$a \leqslant b$，$b \leqslant c \Rightarrow a \leqslant c$

则称 $\leqslant$ 是 P 上的偏序，$\langle P, \leqslant \rangle$ 是一个偏序集。

在偏序集中有最小上界（*lub*）和最大下界（*glb*）的定义，即

定义 10.1.2　设 $\langle P, \leqslant \rangle$ 是一个偏序集，S 是 P 的一个子集，

(1) 如果 $a \in P$ 是 S 的一个上界，而且对于 S 的每个上界 a'，都有 $a \leqslant a'$，则称 a 是 S 的最小上界，或上确界。

(2) 如果 $a \in P$ 是 S 的一个下界，而且对于 S 的每个下界 a'，都有 $a' \leqslant a$，则称 a 是 S 的最大下界，或下确界。

对于有限集 S，偏序关系可以用图形表示。称为哈斯图。规定图形中线段联接的两个点具有关系"$\leqslant$"，并且，位于同一线段下端的点 $\leqslant$ 上端的点，且不存在中间点。用图形表示偏序集比较直观，易于理解，如图 10.1 用图形方式给出几个偏序集。

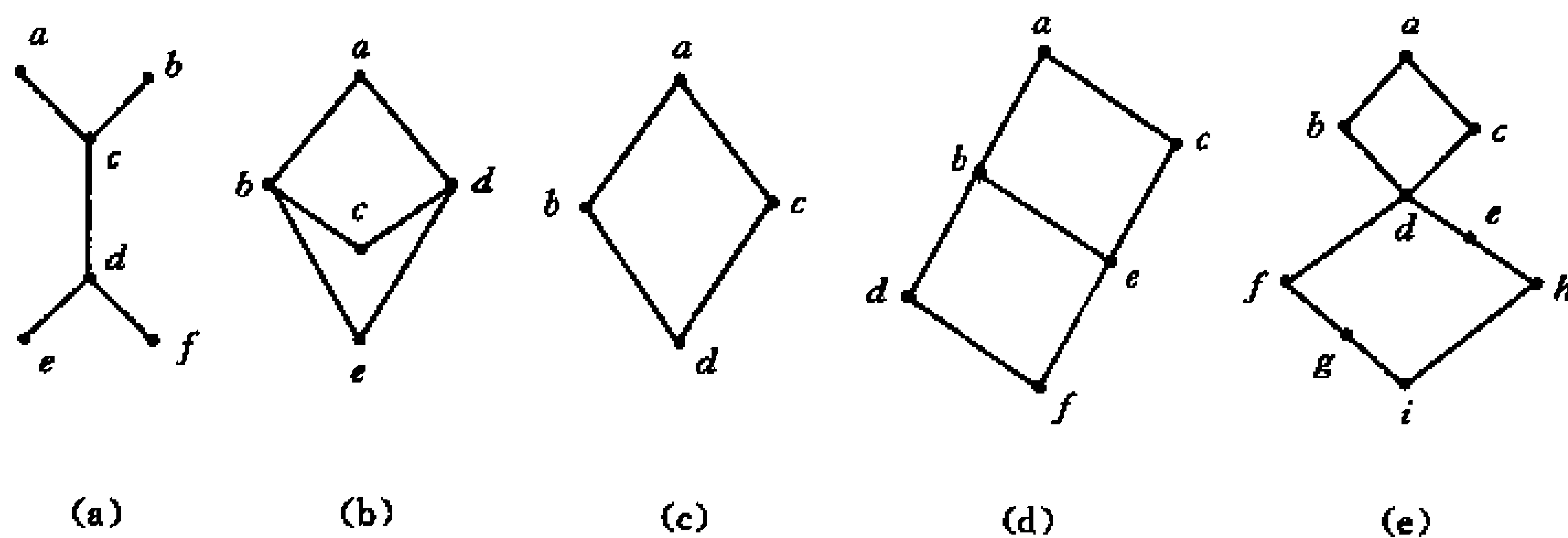


图　10.1

我们知道，对偏序集 P 的任一子集 S 来说，不一定有最小上界或最大下界，如图 10.1 中 (a)，(b)，但是对有些偏序集，它的任一子集确存在最小上界和最大下界，如 (c)，(d)，(e)。这样就引出格的概念。

定义 10.1.3 设 $\langle P, \leqslant\rangle$ 是一个偏序集，如果 P 中的任意两个元素都有最小上界和最大下界，则称 P 关于偏序 $\leqslant$ 构成一个格，记作 $\langle P, \leqslant\rangle$。

例 10.1.1 设 A 是任意集合，则 $\langle \rho(A), \subseteq\rangle$ 是一个格。

证明：容易看出包含关系 $\subseteq$ 是幂集 $\rho(A)$ 中的一个偏序，对任意 $A_1, A_2 \in \rho(A)$，$A_1 \cup A_2$ 是它们的最小上界，$A_1 \cap A_2$ 是最大下界，而且 $A_1 \cup A_2, A_1 \cap A_2 \in \rho(A)$，故 $\rho(A)$ 关于偏序 $\subseteq$ 作成一个格。

例 10.1.2 设 G 是群，$L(G)$ 表示 G 的所有子群构成的集合，$L(G)$ 中的偏序是：对任意 $G_1, G_2 \in L(G)$，$G_1 \leqslant G_2$ 当且仅当 $G_1 \subseteq G_2$。这样对任意 G_1、$G_2 \leqslant G$，G_1 和 G_2 的最小生成子群 $\langle G_1 \cup G_2\rangle$ 是其最小上界，$G_1 \cap G_2$ 是其最大下界。当然 $\langle G_1 \cup G_2\rangle$，$G_1 \cap G_2$ 也是 G 的子群，因此 $\langle L(G), \leqslant\rangle$ 是一个格。

例 10.1.3 设 A 是集合，$\varepsilon(A)$ 为 A 上所有等价关系的集合。则 $\rho \in \varepsilon(A)$ 有 $\rho \subset A \times A$。定义 $\varepsilon(A)$ 上的偏序为 $\delta \leqslant \tau$ 当且仅当 $\delta \subseteq \tau$，则 $\langle \varepsilon(A), \leqslant\rangle$ 是格。

证明：对任意 $\delta, \tau \in \varepsilon(A)$，我们将证明

$glb(\delta, \tau) = \delta \cap \tau$，

$lub(\delta, \tau) = \{(a, b) \mid$ 存在自然数 n，及 $c_1, c_2, \cdots, c_n, c_1 = a, c_n = b, (c_i, c_{i+1}) \in \delta$ 或 $\tau, i = 1, 2, \cdots, n-1\}$。

(1) 对 $glb(\delta, \tau)$，先证 $\delta \cap \tau$ 是等价关系。

(i) 对任意 $a \in A$，$(a, a) \in \delta$，$(a, a) \in \tau$，所以 $(a, a) \in \delta \cap \tau$，自反性成立。

(ii) 对任意 $a, b \in A$，若 $(a, b) \in \delta \cap \tau$，则 $(a. b) \in \delta$，$(a, b) \in \tau$，因为 δ, τ 是等价关系，所以 $(b, a) \in \delta$，$(b, a) \in \tau$，则 $(b, a) \in \delta \cap \tau$，对称性成立。

(iii) 对任意 $a, b, c \in A$，若 $(a, b) \in \delta \cap \tau$，$(b, c) \in \delta \cap \tau$，类似可得 $(a, c) \in \delta \cap \tau$，传递性成立。

其次，因为 $\delta \cap \tau \subseteq \delta, \tau$，所以 $\delta \cap \tau$ 是 δ, τ 的下界。

又对于 δ, τ 任意下界 ρ，$\rho \subseteq \delta$，$\rho \subseteq \tau$，则 $\rho \subseteq \delta \cap \tau$，因此 $\delta \cap \tau$ 是最大下界。

(2) 对 $lub(\delta, \tau)$，令 $\theta = \{(a, b) \mid$ 存在自然数 n 及 $c_1, c_2, \cdots, c_n, c_1 = a, c_n = b, (c_i, c_{i+1}) \in \delta$ 或 $\tau, i = 1, 2, \cdots, n-1\}$。

先证 θ 是等价关系。

(i) 对任意 $a \in A$，令 $n = 2, c_1 = a, c_2 = a$，则有 $(a, a) \in \delta$，所以 $(a, a) \in \theta$，自反性成立。

(ii) 对任意 $a, b \in A$，若 $a, b \in \theta$，则存在 n 及 $c_1, c_2, \cdots, c_n, c_1 = a, c_n = b, (c_i, c_{i-1}) \in \delta$ 或 τ，$i = 1, 2, \cdots, n-1$，因为 δ, τ 是等价关系，所以 $(c_{i+1}, c_i) \in \delta$ 或 τ。

令 $c'_1 = c_n, c'_2 = c_{n-1}, \cdots, c'_n = c_1$，有 $(c'_i, c'_{i+1}) \in \delta$ 或 τ，所以 $(b, a) \in \theta$，对称性成立。

(iii) 对任意 $a, b, c \in A$，若 $(a, b) \in \theta$，$(b, c) \in \theta$，

则有在 $c_1 = a$，c_2，$\cdots$，$c_n = b$，$d_1 = b$，d_2，$\cdots$，$d_m = c$，$(c_i, c_{i+1}) \in \delta$ 或 τ，$(d_i, d_{i+1}) \in \delta$ 或 τ，令 $c_{n+1} = d_1, c_{n+2} = d_2, \cdots, c_{n+m} = d_m$，

则有 $(c_i, c_{i+1}) \in \delta$ 或 τ 对 $i = 1, 2, \cdots, n+m-1$ 成立，所以 $(a, c) \in \theta$ 传递性成立。

其次，对任意$(a,b)\in\delta$，令$n=2$，$c_1=a$，$c_2=b$，则有$(a,b)\in\theta$所以$\delta\subseteq\theta$。同理$\tau\subseteq\theta$，即θ是δ，τ的上界。

又对于δ，τ的任意上界ρ，δ ρ，τ ρ，对任意$(a,b)\in\theta$存在$c_1=a,c_2,\cdots,c_n=b$，$(c_i,c_{i+1})\in\delta$或τ，$i=1,2,\cdots,n-1$，

则 $(c_i,c_{i+1})\in\rho$对$i=1,2,\cdots,n-1$成立．因为ρ是等价关系，所以

$(c_1,c_n)=(a,b)\in\rho$．则$\theta\leqslant\rho$。

因此θ是最小上界。至此，已证明〈ε（A），$\leqslant$〉是格。

在格〈P，$\leqslant$〉中，对任意a，$b\in P$，我们用$a\cup b$表示$\{a,b\}$的最小上界，用$a\cap b$表示$\{a,b\}$的最大下界。因为lub和glb都是唯一确定的，故可以将$\cup$，$\cap$看成是P上的二元运算，因此能够用代数系统（P，$\cup$，$\cap$）表示之。又可把格记作（P，$\cup$，$\cap$），二元运算$\cup$和$\cap$分别称为并运算和交运算。

在格中，对偶原理成立。也就是说，设P是对任意格都为真的一个命题，P'是将P中"$\leqslant$"与"$\geqslant$"，"$\cup$"与"$\cap$"互换的对偶命题，则P'对任意格也为真。这是因为将格L中"$\leqslant$"与"$\geqslant$"互换得到的偏序集仍然是格，其中"$\cup$"与"$\cap$"互换，称为L的对偶格。P对所有格都成立时，其对偶命题对所有对偶格，也即所有格都成立。因此，如果对任意一个格$(L,\leqslant)$，都能证明某个命题为真以后，利用对偶原理，其对偶命题也就不证自立。

下面讨论格的一些基本性质：

定理 10.1.1 在格〈P，$\leqslant$〉中，对任意的a，$b\in P$，都有

$$a\leqslant a\cup b,\qquad b\leqslant a\cup b,$$
$$a\cap b\leqslant a,\qquad a\cap b\leqslant b。$$

证明：因为a和b的并是a的一个上界，所以$a\leqslant a\cup b$，同理$b\leqslant a\cup b$，由对偶原理，可得$a\cap b\leqslant a$，$a\cap b\leqslant b$。

定理 10.1.2 在格〈P，$\leqslant$〉中，对任意a，b，c，$d\in P$，若$a\leqslant b$，$c\leqslant d$，则

$$a\cup c\leqslant b\cup d，a\cap c\leqslant b\cap d。$$

证明：因为$b\leqslant b\cup d$，$d\leqslant b\cup d$，由传递性（$R-3$），可得$a\leqslant b\cup d$，$c\leqslant b\cup d$，由于$a\cup c$是a和c的最小上界，而$b\cup d$是它们的一个上界，因此$a\cup c\leqslant b\cup d$。类似可证$a\cap c\leqslant b\cap d$。

定理 10.1.3 设〈P，$\leqslant$〉是一个格，对任意a，b，$c\in P$，二元运算$\cup$、$\cap$适合以下算律：

$L1$ 幂等律$a\cap a=a$，$a\cup a=a$。

$L2$ 交换律$a\cap b=b\cap a$，$a\cup b=b\cup a$。

$L3$ 结合律$(a\cap b)\cap c=a\cap(b\cap c)$，$(a\cup b)\cup c=a\cup(b\cup c)$。

$L4$ 吸收律$a\cap(a\cup b)=a$，$a\cup(a\cap b)=a$。

证明：

$L1$：由定义，$\{a,a\}$的最小上界就是a，即

$$a\cup a=a,$$

利用对偶原理，即得$a\cap a=a$。

$L2$：因为 $\{a, b\} = \{b, a\}$，所以 $L2$ 成立。

$L3$：由定理 10.1.1

$(a\cap b)\cap c\leqslant a\cap b\leqslant b, (a\cap b)\cap c\leqslant a\cap b\leqslant a, (a\cap b)\cap c\leqslant c$。

由定理 10.1.2，有 $(a\cap b)\cap c\leqslant b\cap c$，

以及 $(a\cap b)\cap c\leqslant a\cap(b\cap c)$。

同理可证 $a\cap(b\cap c)\leqslant(a\cap b)\cap c$，

由反对称性，故得 $a\cap(b\cap c)=(a\cap b)\cap c$。

利用对偶原理，有

$$(a\cup b)\cup c=a\cup(b\cup c)。$$

$L4$：由定理 10.1.1 得到 $a\leqslant a\cup(a\cap b)$。

由于 $a\cap b\leqslant a$ 和 $a\leqslant a$，根据定理 10.1.2，有

$$(a\cap b)\cup a\leqslant a,$$

因此

$$a=a\cup(a\cap b)。$$

由对偶原理

$$a=a\cap(a\cup b)。$$

人们自然要问，如果一个代数系统 $(S, \cup, \cap)$ 适合算律 $L1\sim L4$，那么能否在集合 S 中适当地定义一个偏序 $\leqslant$，使得 $(S, \leqslant)$ 成为一个格呢？下面定理回答了这个问题。

定理 10.1.4 设代数系统 $(S, \cup, \cap)$ 中的二元运算都适合算律 $L2\sim L4$，则可以定义一个偏序 $\leqslant$，满足对任意 $a, b\in S$，$a\cup b$ 是其最小上界，$a\cap b$ 是其最大下界，即 $(S, \leqslant)$ 是格。

注意，定理中没有提到幂等律 $L1$，这是因为吸收律 $L4$ 已蕴含了 $L1$：

$$a\cup a=a\cup(a\cap(a\cup a))=a\cup(a\cap b)=a。$$

其中 $b=a\cup a\in S$。以下证明该定理。

证明：在 S 中规定关系"$\leqslant$"如下：对任意 $a, b\in S$，$a\leqslant b$ 当且仅当 $a\cup b=b$，先证明 $\leqslant$ 是一个偏序。

1. 自反性，对任意 $a\in S$，由 $L1$ 知 $a\cup a=a$，于是有 $a\leqslant a$。

2. 反对称性，对任意 $a, b\in S$，若 $a\leqslant b$，$b\leqslant a$，则 $a\cup b=b$，$b\cup a=a$，所以由 $L2$ 知 $a=b\cup a=a\cup b=b$。

3. 传递性，对任意 $a, b, c\in S$，若 $a\leqslant b$，$b\leqslant c$，则 $a\cup b=b$，$b\cup c=c$，于是由 $L3$ 得

$$a\cup c=a\cup(b\cup c)=(a\cup b)\cup c=b\cup c=c,$$

即 $a\leqslant c$，故传递性成立。

下面再证对任意 $a, b\in S$，都存在最大下界 $a\cap b$ 和最小上界 $a\cup b$。要证 $a\cap b$ 是最大下界，只要证明 $a\cap b$ 满足 (1)，(2) 即可。

(1) $a\cap b\leqslant a$，$a\cap b\leqslant b$。

(2) 对任意 $x\in S$，若 $x\leqslant a$，$x\leqslant b$，则 $x\leqslant a\cap b$。

由所规定的 $\leqslant$ 关系，$a\leqslant b$ 当且仅当 $a\cup b=b$，可以得到，若 $a\cup b=b$，则由 $L4$，$a\cap b=$

$a\cap(a\cup b)=a$；同时若 $a\cap b=a$，则 $a\cup b=b\cup a=b\cup(b\cap a)=b$。因此有 $a\leqslant b$ 当且仅当 $a\cap b=a$。这样由

$$(a\cap b)\cap a=a\cap(a\cap b)=(a\cap a)\cap b=a\cap b,$$

故 $a\cap b\leqslant a$，同理可证 $a\cap b\leqslant b$。

任取 $x\in S$，设 $x\leqslant a$，$x\leqslant b$，有 $x\cap a=x$，$x\cap b=x$，于是

$$x\cap(a\cap b)=(x\cap a)\cap b=x\cap b=x,$$

故 $x\leqslant a\cap b$。

因此 $a\cap b$ 是 $\{a, b\}$ 的最大下界。类似可证 $a\cup b$ 是其最小上界。

综上可证 $\langle S, \leqslant\rangle$ 是一个格。

因此，若代数系统 $(S, \cup, \cap)$ 中的二元运算 $\cup$，$\cap$ 适合 $L1\sim L4$，我们也称 $(S, \cup, \cap)$ 是一个格。由此可以看出格即可从偏序集定义，又可从代数运算定义，这是格的特殊性。

例 10.1.4 设 Z_+ 是正整数集，对任意 $a, b\in Z_+$，规定 $a\cup b=[a, b]$，即 a 与 b 的最小公倍数，$a\cap b=(a, b)$，即 a 与 b 的最大公约数。显然 $\cup$，$\cap$ 是 Z_+ 上的二元运算．同时由于

(1)$a\cap a=(a,a)=a, a\cup a=[a,a]=a$。

(2)$a\cap b=(a,b)=(b,a)=b\cap a$，

$a\cup b=[a,b]=[b,a]=b\cup a$。

(3)$(a\cap b)\cap c=((a,b),c)=(a,(b,c))=a\cap(b\cap c)$，

$(a\cup b)\cup c=[[a,b],c]=[a,[b,c]]=a\cup(b\cup c)$。

(4)因 $a\mid[a,b]$，故

$$a\cap(a\cup b)=(a,[a,b])=a。$$

因 $(a,b)\mid a$，故

$$a\cup(a\cap b)=[a,(a,b)]=a。$$

即 $(Z_+, \cup, \cap)$ 满足算律 $L1\sim L4$，所以 $\langle Z_+, \leqslant\rangle$ 是一个格。

例 10.1.5 设 G 是 Klein 四元群，$G=\{e, a, b, ab\}$，$L(G)=\{I, H_1, H_2, H_3, G\}$，其中 $H_1=\{e, a\}$，$H_2=\{e, b\}$，$H_3=\{e, ab\}$。$H\cap K$ 表示子群 H 与 K 的交，$H\cup K$ 表示由 H 和 K 生成的子群，则 $(L(G), \cup, \cap)$ 是一个格。

证明：显见 $L(G)$ 包含了 G 的全部子群，$\cup$ 和 $\cap$ 是 $L(G)$ 上的二元运算，现只要证明 $\cup$，$\cap$ 运算适合 $L1\sim L4$ 即可。

对任意 $K_1, K_2, K_3\in L(G)$，显然

$K_1\cap K_1=K_1, K_1\cup K_1=K_1$，

$K_1\cap K_2=K_2\cap K_1, K_1\cup K_2=K_2\cup K_1$，

$(K_1\cap K_2)\cap K_3=K_1\cap(K_2\cap K_3)$，

$(K_1\cup K_2)\cup K_3=K_1\cup(K_2\cup K_3)$。

对算律 $L4$，因为 $K_1\subseteq K_1\cup K_2, K_1\cap K_2\subseteq K_1$，所以

$K_1\cap(K_1\cup K_2)=K_1$，　$K_1\cup(K_1\cap K_2)=K_1$。

故此 $\langle L(G), \cup, \cap\rangle$ 是一个格。$L(G)$ 关于 $\cup$，$\cap$ 的运算表如下：

$\cup$	I	H_1	H_2	H_3	G
I	I	H_1	H_2	H_3	G
H_1	H_1	H_1	G	G	G
H_2	H_2	G	H_2	G	G
H_3	H_3	G	G	H_3	G
G	G	G	G	G	G

$\cap$	I	H_1	H_2	H_3	G
I	I	I	I	I	I
H_1	I	H_1	I	I	H_1
H_2	I	I	H_2	I	H_2
H_3	I	I	I	H_3	H_3
G	I	H_1	H_2	H_3	G

关于格，还有以下几个基本定理：

定理 10.1.5 设〈P，$\leqslant$〉是一个格，对任意 a，b，$c\in P$，都有

$$a\cup(b\cap c)\leqslant(a\cup b)\cap(a\cup c)。$$

$$(a\cap b)\cup(a\cap c)\leqslant a\cap(b\cup c)。$$

证明：由于 $a\leqslant a\cup b$，$a\leqslant a\cup c$，所以

$$a\leqslant(a\cup b)\cap(a\cup c)。$$

另外，由于 $b\cap c\leqslant b\leqslant a\cup b$，$b\cap c\leqslant c\leqslant a\cup c$，所以

$$b\cap c\leqslant(a\cup b)\cap(a\cup c)。$$

由定理 10.1.2，即得

$$a\cup(b\cap c)\leqslant(a\cup b)\cap(a\cup c)。$$

根据对偶原理又得

$$(a\cap b)\cup(a\cap c)\leqslant a\cap(b\cup c)。$$

定理 10.1.6 设〈P，$\leqslant$〉是一个格，对任意的 a，$b\in P$，都有

$$a\leqslant b<=>a\cap b=a<=>a\cup b=b。$$

该定理的证明留给读者练习。

定理 10.1.7 设〈P，$\leqslant$〉是一个格，则对任意 a，b，$c\in P$，有

$$a\leqslant c<=>a\cup(b\cap c)\leqslant(a\cup b)\cap c。$$

证明：必要性。由定理 10.1.6 知

$$a\leqslant c<=>a\cup c=c。$$

由定理 10.1.5 得到

$$a\cup(b\cap c)\leqslant(a\cup b)\cap(a\cup c)。$$

将$(a\cup c)$用 c 代入，有

$$a\cup(b\cap c)\leqslant(a\cup b)\cap c。$$

充分性。若$a\cup(b\cap c)\leqslant(a\cup b)\cap c$，显然有

$$a\leqslant a\cup(b\cap c)\leqslant(a\cup b)\cap c\leqslant c。$$

即 $a\leqslant c$，所以

$$a\leqslant c<=>a\cup(b\cap c)\leqslant(a\cup b)\cap c。$$

定理 10.1.7 中的不等式通称为模不等式，利用它还可以推出下述方法表示的模不等式

$$(a\cap b)\cup(a\cap c)\leqslant a\cap(b\cup(a\cap c))，$$

$$a\cup(b\cap(a\cup c))\leqslant(a\cup b)\cap(a\cup c)。$$

定理 10.1.8 设$<P，\leqslant>$是一个格，则对任意 a，b，c，$d\in P$，有

$$(a\cap b)\cup(c\cap d)\leqslant(a\cup c)\cap(b\cup d)。$$

证明：因为 $(a\cap b)\leqslant a\leqslant a\cup c,(a\cap b)\leqslant b\leqslant b\cup d$，

所以 $(a\cap b)\leqslant(a\cup c)\cap(b\cup d)$。

又因为 $(c\cap d)\leqslant c\leqslant a\cup c,(c\cap d)\leqslant d\leqslant b\cup d$，

所以 $(c\cap d)\leqslant(a\cup c)\cap(b\cup d)$。

因此由定理 10.1.2，$(a\cap b)\cup(c\cap d)\leqslant(a\cup c)\cap(b\cup d)$。

定理 10.1.8 还有下面重要推广。

定理 10.1.9 设 $<P,\leqslant>$ 是一个格，$a_{ij}\in P$，$1\leqslant i\leqslant n$，$1\leqslant j\leqslant m$，则有

$$\bigcup_{j=1}^{m}(\bigcap_{i=1}^{n}a_{ij})\leqslant\bigcap_{i=1}^{n}(\bigcup_{j=1}^{m}a_{ij})$$

证明留给读者练习。

10.2 子格、同态与同构

对于任何代数系统 S，都有其子系统 S' 的概念。由于格也是一个代数系统，因此也有子格的概念。

定义 10.2.1 设 $(S,\cup,\cap)$ 是一个格，T 是 S 的非空子集，若 T 关于二元运算 $\cup$，$\cap$ 也是封闭的，则称 T 是 S 的一个子格。

注意，定义中所讲的“封闭”，不仅仅讲 T 本身是封闭的，而且还与 S 有关，也就是说，对任意 a，$b\in T$，如果在 S 中 $a\cup b=c$，$a\cap b=d$，则 $c\in T$，$d\in T$，否则我们不能讲 T 是 S 的子格。

例 10.2.1 设 Z_+ 是正整数集，T 是其中的偶数集，$\cup$，$\cap$ 运算分别是求最小公倍数和最大公约数。由于任意两个偶数的最小公倍数和最大公约数也都是偶数，故 T 关于 $\cup$，$\cap$ 运算都是封闭的，即 T 是 $(Z_+,\cup,\cap)$ 的一个子格。

例 10.2.2 设 $S=\{1,2,3,5,6,10,15,30\}$，$\cup$，$\cap$ 分别是求最小公倍数和最大公约数的运算，则 $(S,\cup,\cap)$ 是一个格，其图示如 10.2 (a)。$T_1=\{1,2,5,10\}$，它也是一个格，而且是 S 的一个子格。$T_2=\{1,2,3,10,30\}$ 也是一个格，而且 T_2S，但是 T_2 不是 S 的子格，因为在 S 中 $[2\cup3]=6$，而在 T_2 中，$[2\cup3]=30$。这就不能说 T_2 关于 S 中的运算保持封闭。因此 T_2 虽然是一个格，但不是 S 的子格。

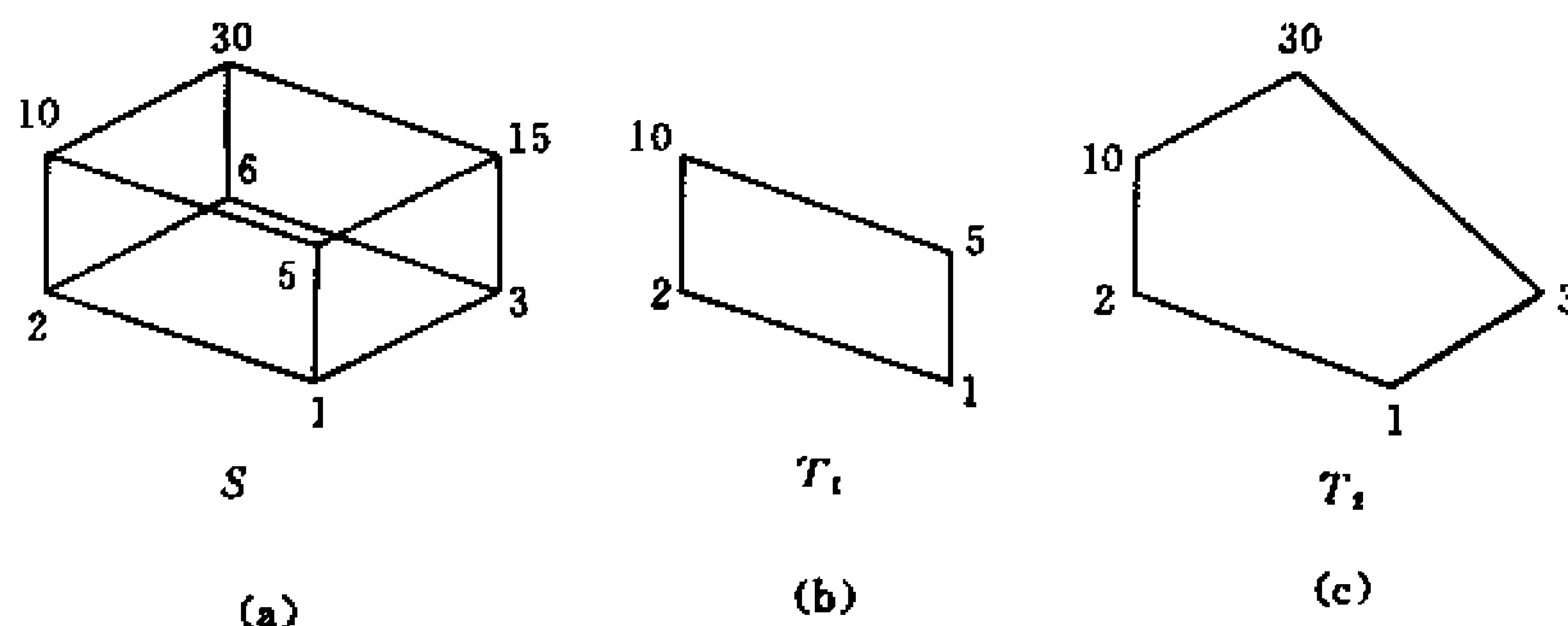


图 10.2

定理 10.2.1 T 是格 S 的一个子格，则 T 对于格 S 的二元运算 $\cup$、$\cap$ 也构成一个格。

证明：由于 T 关于二元运算 $\cup$，$\cap$ 是封闭的，且 $\cup$，$\cap$ 在 S 中适合算律 $L1 \sim L4$，故 T 关于 $\cup$，$\cap$ 运算也适合算律 $L1 \sim L4$。因此 $(T, \cup, \cap)$ 也是一个格。

例 10.2.3 设 $\langle S, \leqslant \rangle$ 是一个格，$a \in S$，令

$$T = \{x \in S \mid x \leqslant a\},$$

则 T 是 S 的一个子格。

证明：因为 $a \leqslant a$，故 T 非空。对任意 x，$y \in T$，由 $x \leqslant a$，$y \leqslant a$ 可知

$$x \cup y \leqslant a, \quad x \cap y \leqslant a。$$

即 $x \cup y \in T$，$x \cap y \in T$，所以 T 关于二元运算 $\cup$，$\cap$ 封闭，即 T 是 S 的子格。

例 10.2.4 设 $(S, \cup, \cap)$ 是一个格，a，$b \in S$，且 $a \leqslant b$，令

$$T = \{x \in S \mid a \leqslant x \leqslant b\},$$

则 T 是 S 的一个子格。

证明：因为 $a \leqslant a$，$a \leqslant b$，故 $a \in T$，即 T 非空对任意 x，$y \in T$，由 $a \leqslant x \leqslant b$，$a \leqslant y \leqslant b$ 可知

$$a \leqslant x \cup y \leqslant b, \quad a \leqslant x \cap y \leqslant b。$$

即 $x \cup y \in T$，$x \cap y \in T$，故 T 关于二元运算 $\cup$ 和 $\cap$ 都是封闭的，所以 T 是 S 的子格，该子格亦称为 S 的一个闭区间，记为 b/a。

例如 图 10. 1 (*e*) 中，$T_1 = \{b, d, e, f, g, h, i\}$ 是一个子格，它满足 $T_1 = \{x \mid i \leqslant x \leqslant b\}$；$T_2 = \{b, d, f, g\}$ 也是一个子格，它满足 $T_2 = \{x \mid g \leqslant x \leqslant b\}$。

再以下介绍关于格的积代数的概念。

定义 10.2.2 设 $(S, \cup, \cap)$ 和 $(L, \oplus, *)$ 是两个格，可以由它们导出一个代数系统 $(S \times L, +, \times)$，其中 $+$ 和 $\times$ 是 $S \times L$ 中的二元运算，对于任意 $\langle a_1, b_1 \rangle$，$\langle a_2, b_2 \rangle \in S \times L$，都有

$$\langle a_1, b_1 \rangle + \langle a_2, b_2 \rangle = \langle a_1 \cup a_2, b_1 \oplus b_2 \rangle。$$

$$\langle a_1, b_1 \rangle \times \langle a_2, b_2 \rangle = \langle a_1 \cap a_2, b_1 * b_2 \rangle。$$

这时称 $(S \times L, +, \times)$ 是格 $(S, \cup, \cap)$ 和 $(L, \oplus, *)$ 的直积或积代数。

在该定义中，运算 $+$ 和 $\times$ 是由运算 $\cup$，$\cap$ 和 $\oplus$，$*$ 来定义的，因此它一定是可交换的，可结合的，同时满足吸收律，亦即积代数也是一个格。当然，一般来说，积代数 $S \times L$ 比 S 和 L 的势要大，这样我们可以用积代数构造更大的格。

例 10.2.5 设 $S = \{0, 1\}$，在图 10. 3 中分别给出了格 $\langle S, \leqslant \rangle$，$\langle S^2, \leqslant_2 \rangle$ 和 $\langle S^3, \leqslant_3 \rangle$ 的图形。

推而广之，在格 $\langle S^n, \leqslant_n \rangle$ 中，其元素是 $\langle a_1, a_2, \cdots, a_n \rangle$，其中 $a_i = 0$ 或 1 $(i=1, 2, \cdots, n)$。对于任意 a，$b \in S^n$，$a = \langle a_1, a_2, \cdots, a_n \rangle$，$b = \langle b_1, b_2, \cdots, b_n \rangle$，有

$$a \leqslant_n b \Leftrightarrow a_i \leqslant b_i, \quad i = 1, 2, \cdots, n。$$

当然，格 $\langle S^n, \leqslant_n \rangle$ 的哈斯图应是一个 n 维的立方体。

例 10.2.6 设 $S = \{1, 2, 4\}$，$L = \{1, 2, 3, 6\}$，S，L 中的偏序关系都是整除关系，因此它们都是格。其积代数 $L \times S$ 也是格，如图 10.4 所示

由于格是一个代数系统，因此同样也有关于格的同态的定义。

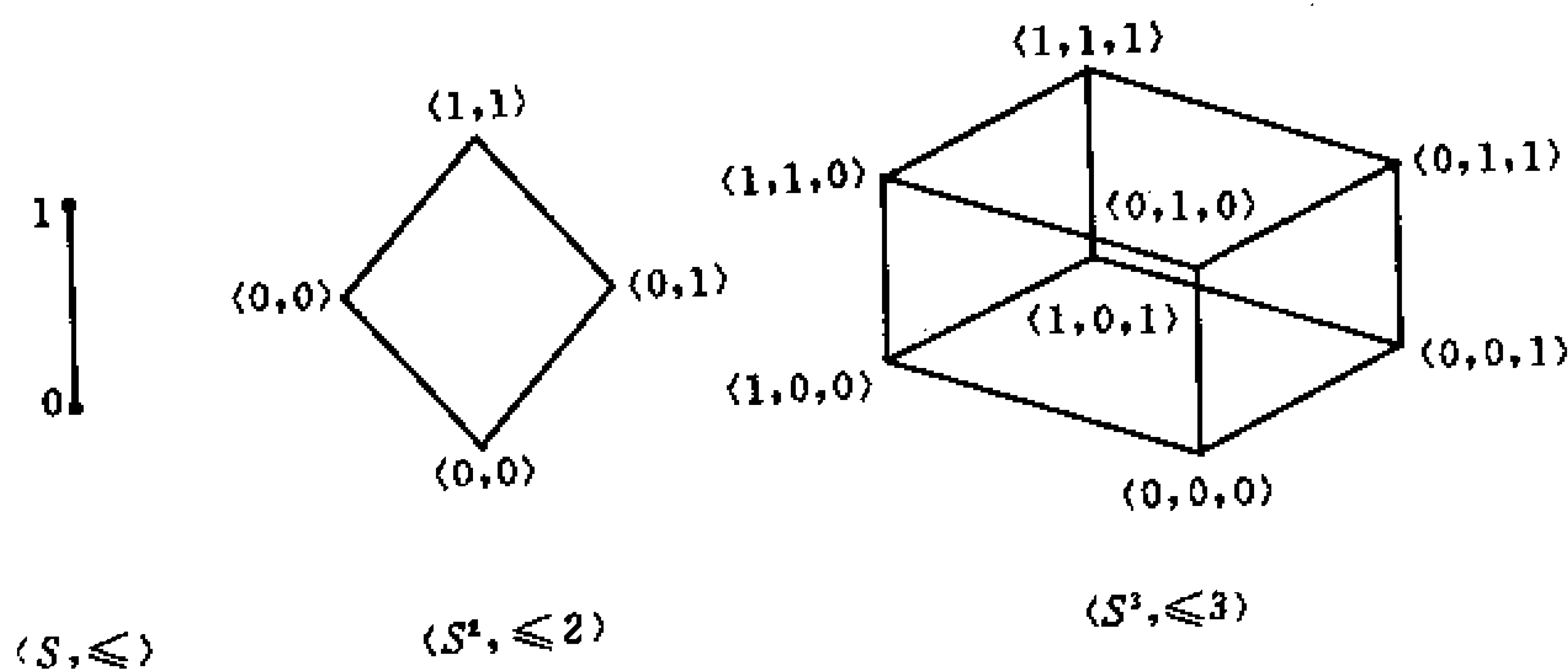


图 10.3

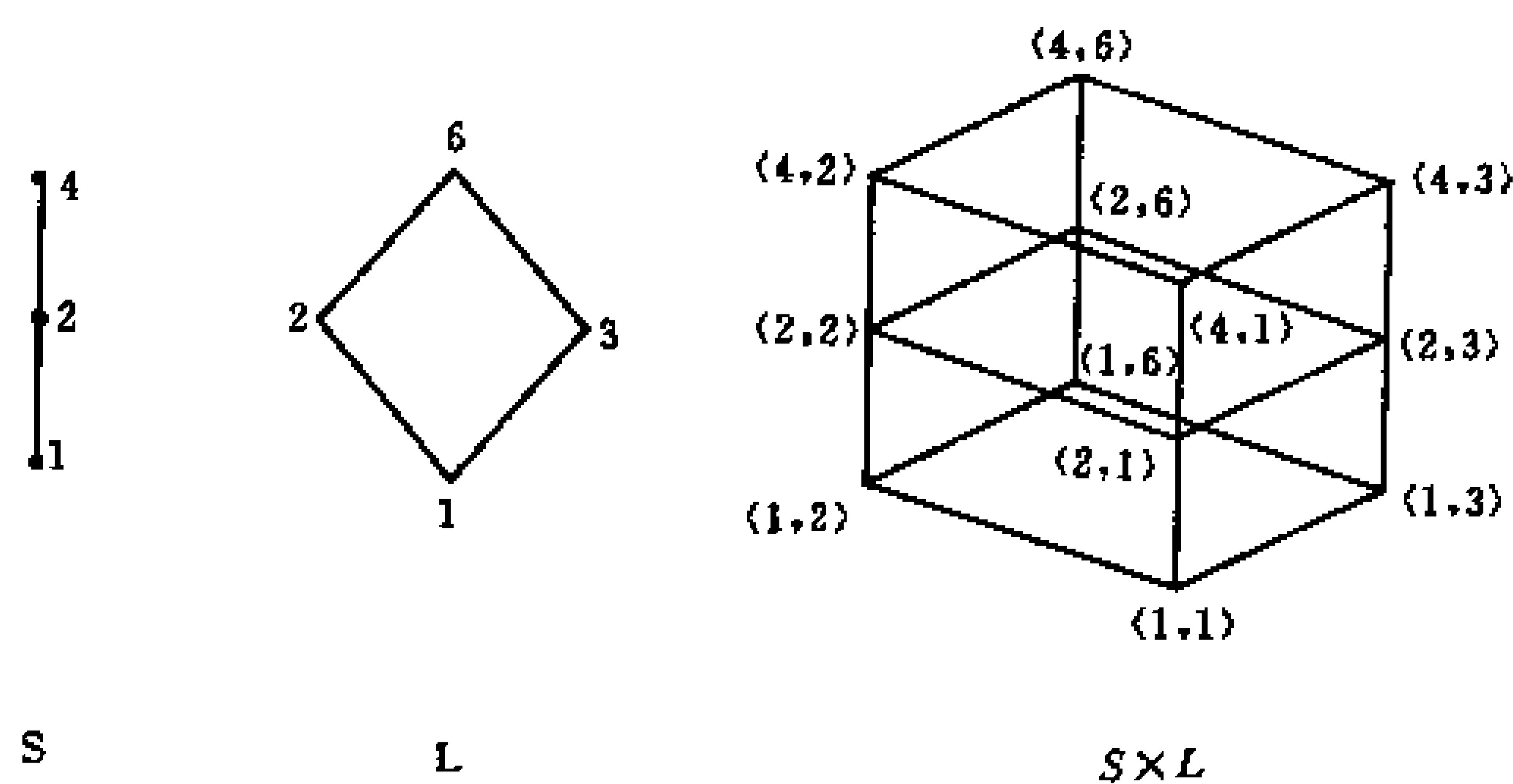


图 10.4

定义 10.2.3 设 S，S'是两个格，如果存在 S 到 S'的一个映射 φ，使得对任意 a，$b\in S$，有

若 $a\leqslant b$，则 $\varphi(a)\leqslant\varphi(b)$，此时称 φ 为 S 到 S'的保序映射；

若 $\varphi(a\cup b)=\varphi(a)\cup\varphi(b)$，称 φ 为 S 到 S'的保并同态；

若 $\varphi(a\cap b)=\varphi(a)\cap\varphi(b)$，称 φ 为 S 到 S'的保交同态；

若 φ 即是保并同态，又是保交同态，则称 φ 为 S 到 S'的格同态。

当 φ 是单射或满射时，又可称 φ 是单同态或满同态。用符号 $S\sim S'$表示满同态。

定义 10.2.3 中的四种同态有下面关系：

定理 10.2.2 若 φ 是格同态，则它即是保并同态，又是保交同态；若 φ 是保并同态或保交同态，则 φ 是保序映射。

证明：定理前半部分即为格同态的定义。下面证明后半部分。

若 φ 是保并同态，φ: $S\to S'$，对任意 $a,b\in S$，$a\leqslant b$，

有 $b=a\cup b$

$\varphi(b)=\varphi(a\cup b)=\varphi(a)\cup\varphi(b)$，得

$\varphi(a)\leqslant\varphi(b)$，所以 φ 是保序映射。

类似可证若 φ 是保交同态，则 φ 是保序映射。

要注意上面四种同态是互不相同的，可从下面例子看出。

例 10.2.7 图 10.5 中，$\langle S,\leqslant\rangle$ 是一个格，其中 $S=\{a,b,c,d,e\}$。当然，$\langle\rho(S),\leqslant\rangle$ 也是一个格。

在 S 到$\rho(S)$之间构造一个映射 φ:使得对任意 $x\in S$,有

$$f(x)=\{y\in S\mid y\leqslant x\}。$$

这样

$$f(a)=S,f(b)=\{b,e\},f(c)=\{c,e\},$$
$$f(d)=\{d,e\},f(e)=\{e\}。$$

此时,当 x,$y\in S$ 且 $x\leqslant y$ 时,满足 $f(x)\leqslant f(y)$,所以 f 是保序映射。但是 f 并不是 S 到 $\rho(S)$的保并同态。比如,对 c,$d\in S$,$c\cup d=a$,因此 $f(c\cup d)=f(a)=S$,而 $f(c)\cup f(d)=\{c,d,e\}$,因此 $f(c\cup d)\neq f(c)\cup f(d)$。而 φ 却是保交的,当 $x\leqslant y$ 时 $\varphi(x\cap y)=\varphi(x)\cap\varphi(y)$易验证,再验证 $f(b\cap c)=f(e)=\{e\},f(b)\cap f(c)=\{b,e\}\cap\{c,e\}=\{e\}$,相等。类似 $f(b\cap d)$,$f(c\cap d)$也保持运算,所以 φ 保交。

例 10.2.8 S 仍为图 10.5 中的格,S'为五个元素 a',b',c',d',e'构成的链,$e'\leqslant d'\leqslant c'\leqslant b'\leqslant a'$。$\varphi$ 是 S 到 S' 的映射,$\varphi(a)=a'$,$\varphi(b)=b'$,$\varphi(c)=c'$,$\varphi(d)=d'$,$\varphi(e)=e'$。易证 φ 是保序映射,但 $\varphi(b\cap c)=\varphi(e)=e'\neq c'=\varphi(b)\cap\varphi(c)$,$\varphi(b\cup c)=\varphi(a)=a'\neq b'=\varphi(b)\cup\varphi(c)$,所以 φ 不保并,也不保交。

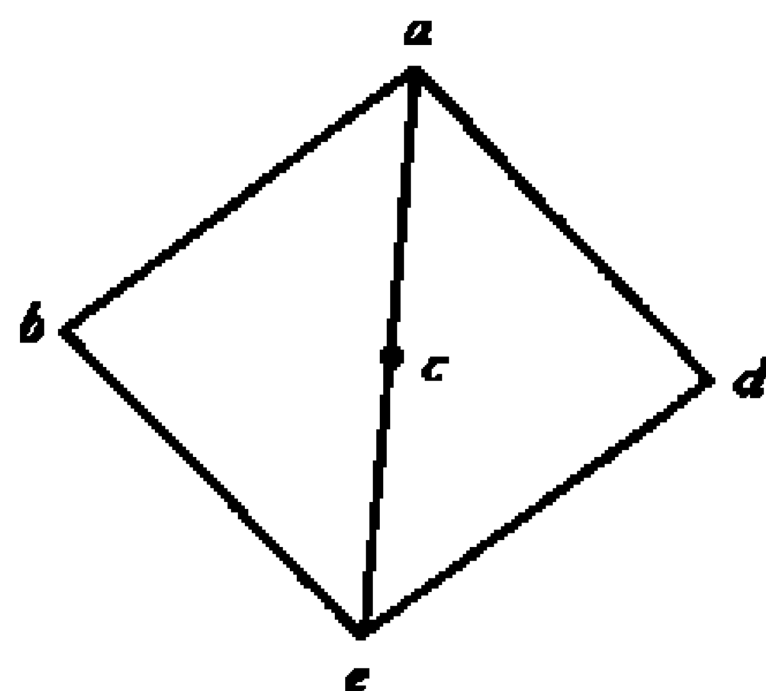


图 10.5

当 φ 是双射时,与同态概念类似地又有同构概念。

定义 10.2.4 设 S,S'是两个格,如果存在 S 到 S'的一个双射 φ,使得对任意 a,$b\in S$,有

$a\leqslant b$ 当且仅当 $\varphi(a)\leqslant\varphi(b)$,称 φ 为 S 到 S' 的保序同构。

$\varphi(a\cup b)=\varphi(a)\cup\varphi(b)$,称 φ 为 S 到 S' 的保并同构。

$\varphi(a\cap b)=\varphi(a)\cap\varphi(b)$,称 φ 为 S 到 S' 的保交同构。

若 φ 即是保交同构又是保并同构,则称 φ 是 S 到 S' 的格同构。用符号 $S\cong S'$ 表示格同构。

例 10.2.9 设 $A=\{a,b,c\}$,则$(\rho(A),\cup,\cap)$是一个格,它与例 10.2.2 中的 S 是同构的。

证明:因为 $\rho(A)=\{\varnothing,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},A\}$,它与 S 中元素数目相同。我们在 $\rho(A)$和 S 之间确定一个双射 φ:$x_i\to y_i$,x_i,y_i 分别是 $\rho(A)$与 S 中的第 i 个元素。于是对任意 $x_i,x_j\in\rho(A)$,容易验证

$$\varphi(x_i\cup x_j)=[y_i,y_j]=y_i\cup y_j=\varphi(x_i)\cup\varphi(x_j),$$
$$\varphi(x_i\cap x_j)=(y_i,y_j)=y_i\cap y_j=\varphi(x_i)\cap\varphi(x_j)。$$

因此 $\rho(A)\cong S$。

定义 10.2.4 所定义的四种同构的关系与定义 10.2.3 中四种同态的关系不同。有下面定理。

定理 10.2.3 设 φ 是格 S 到 S'的映射,则 φ 是格同构等价于它是保交同构,也等价于它是保并同构,也等价于它是保序同构,也即定义 10.2.4 中四种同构相互等价。

证明:只要证明保序同构等价于保交同构,完全类似地就可证明保序同构等价于保并同构,从而保序同构等价于格同构,也即四种同构等价。

若已知 φ 是保序同构,即对所有 $a,b\in S$,$a\leqslant b$ 当且仅当 $\varphi(a)\leqslant\varphi(b)$,

则对任意 $a, b\in S$，$a\cap b\leqslant a$，$a\cap b\leqslant b$，所以 $\varphi(a\cap b)\leqslant\varphi(a)$，$\varphi(a\cap b)\leqslant\varphi(b)$，$\varphi(a\cap b)\leqslant\varphi(a)\cap\varphi(b)$，又因 φ 是双射，则存在 $x\in S$，$\varphi(x)=\varphi(a)\cap\varphi(b)$，而 $\varphi(x)\leqslant\varphi(a)$，$\varphi(x)\leqslant\varphi(b)$ 所以 $x\leqslant a$，$x\leqslant b$，$x\leqslant a\cap b$，则 $\varphi(a)\cap\varphi(b)=\varphi(x)\leqslant\varphi(a\cap b)$，因此 $\varphi(a)\cap\varphi(b)=\varphi(a\cap b)$，即 φ 是保交同构。

反之，若以知 φ 是保交同构，即对所有 $a, b\in S$，$\varphi(a)\cap\varphi(b)=\varphi(a\cap b)$，则对任意 $a, b\in S$，若 $a\leqslant b$，则有 $a=a\cap b$，$\varphi(a)=\varphi(a\cap b)=\varphi(a)\cap\varphi(b)$，得到 $\varphi(a)\leqslant\varphi(b)$，若 $\varphi(a)\leqslant\varphi(b)$，则有 $\varphi(a)=\varphi(a)\cap\varphi(b)=\varphi(a\cap b)$，因 φ 是双射，从而有 $a=a\cap b$，$a\leqslant b$，所以 φ 是保序同构。证毕。

10.3 分配格与有补格

在定理 10.1.5 中已经指出，在格 S 中的任意三个元素 a，b，c 之间，都存在下述关系

$$a\cup(b\cap c)\leqslant(a\cup b)\cap(a\cup c),$$

$$(a\cap b)\cup(a\cap c)\leqslant a\cap(b\cup c)。$$

也就是说，它并不要求∪、∩运算之间适合分配律，但是有一些格的确满足分配律，这样的格叫做分配格。

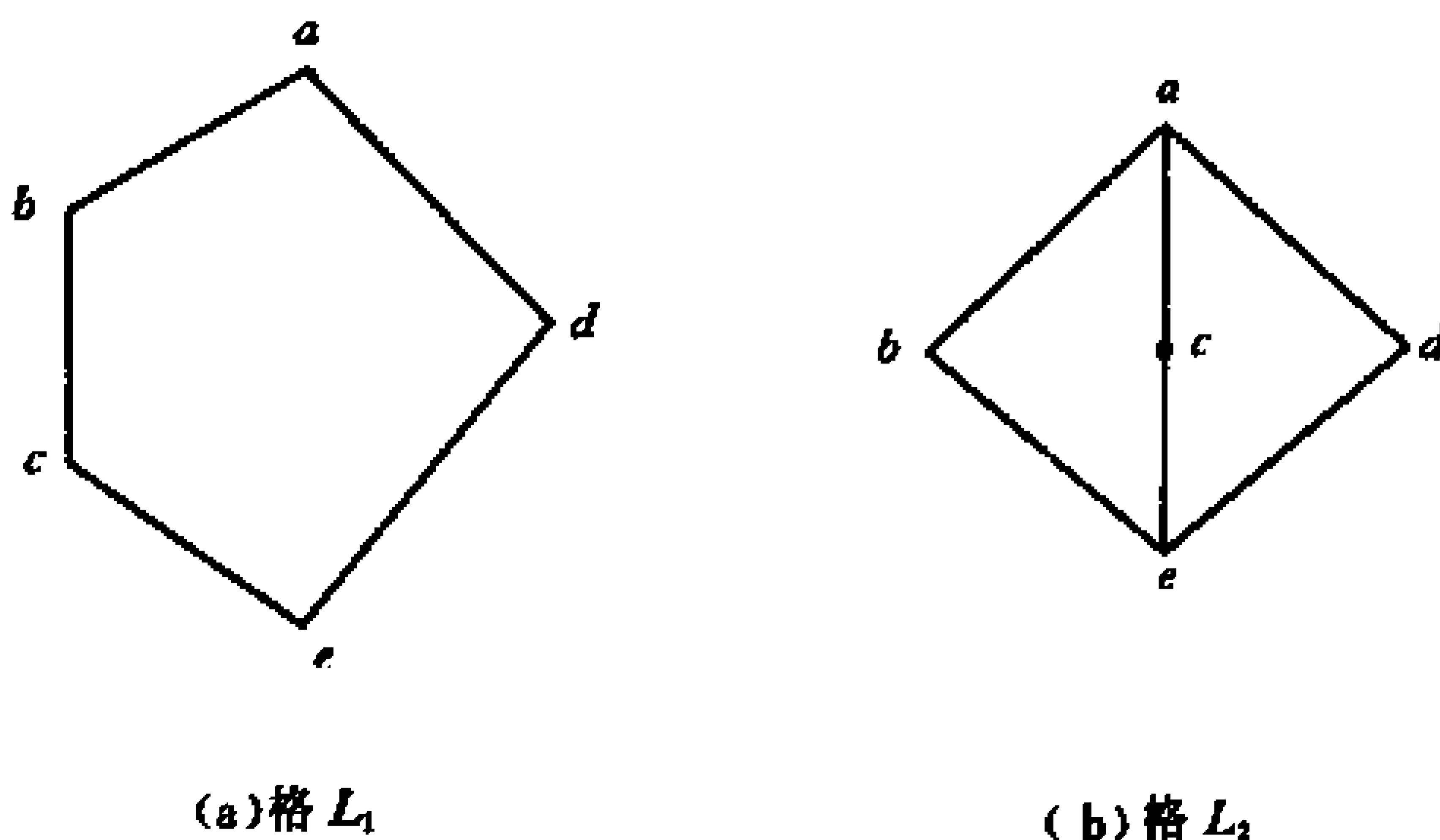
在介绍分配格以前，我们首先介绍一类条件比分配格弱的但也很有用的格：模格。定理 10.1.7 给出了格所满足的模不等式，将不等式变为等式，就得到模格。

定义 10.3.1 设 $(S,\cup,\cap)$ 是一个格，对任意 a，b，$c\in S$，若 $b\leqslant a$，就有

$$a\cap(b\cup c)=b\cup(a\cap c)。$$

成立，则称 $(S, \cup, \cap)$ 是模格。该等式又称模律。

例 10.3.1 图 10.6（a）中的格 $L1$ 不是模格，而图（b）中的格 $L2$ 是模格。



(a)格 L_1　　　(b)格 L_2

图 10.6

证明：在格 $L1$ 中，$c\leqslant b$，而 $c\cup(b\cap d)=c\cup e=c$，

$$b\cap(c\cup d)=b\cap a=b。$$

所以 $c\cup(b\cap d)\neq b\cap(c\cup d)$，$L1$ 不是模格。

在格 $L2$ 中，取 e，b，c，$e\leqslant b$，

$$e\cup(b\cap c)=e\cup e=e=b\cap c=b\cap(e\cup c)。$$

满足模律，对其它情况也可类似验证，最后可知格 $L2$ 是模格。

图 10.6 中两个格是很重要的很有代表性的两个格。后面我们将会谈到它们的作用。

例 10.3.2 设 G 是一个群，则 G 的一切正规子群作成的格 $N(G)$ 是模格。

证明：显然 $N(G)$ 非空，设任意 H_1，H_2，$H_3 \in N(G)$，且 $H_2 \subseteq H_1$，任取 $a \in H_2 \cup (H_1 \cap H_3)$，要证 a 也属于 $H_1 \cap (H_2 \cup H_3)$，即

$$H_2 \cup (H_1 \cap H_3) \subseteq H_1 \cap (H_2 \cup H_3)。$$

因为 $a \in H_2 \cup (H_1 \cap H_3)$，则 $a = k_2 k$，其中 $k_2 \in H_2$，$k \in H_1 \cap H_3$，由于 $H_2\ H_1$，故 $k_2 k \in H_1$；又因 $k_2 \in H_2$，$k \in H_3$，所以 $k_2 k \in H_2 \cup H_3$，即 $a \in H_1 \cap (H_2 \cup H_3)$，故 $H_2 \cup (H_1 \cap H_3) \subseteq H_1 \cap (H_2 \cup H_3)$。

反之，若 $a \in H_1 \cap (H_2 \cup H_3)$，因为 $a \in H_1$，令 $a = h_1$，又因为 $a \in H_2 \cup H_3$，令 $a = h_2 h_3$，则 $h_1 = h_2 h_3$，于是 $h_2^{-1} h_1 = h_3$，由于 H_1 是正规子群，所以 $h_3 \in H_1$，即 $h_3 \in H_1 \cap H_3$。因此 $h_2 h_3 \in H_2 \cup (H_1 \cap H_3)$，即 $a \in H_2 \cup (H_1 \cap H_3)$。

所以
$$H_1 \cap (H_2 \cup H_3) \subseteq H_2 \cup (H_1 \cap H_3)。$$

综上，得证。

从此例可以看出，模格的概念有其实际背景。事实上，模格的许多性质在代数中也有很好的应用，但这方面本书不再作更多介绍。

下面给出模格的判定方法。

定理 10.3.1 设 S 是一个格，则 S 是模格的充要条件是对任意 a，b，$c \in S$，若 $b \leqslant a$，$a \cup c = b \cup c$，$a \cap c = b \cap c$，则 $a = b$。

证明：必要性。若 S 是模格，则对任意 a，b，$c \in S$，若 $b \leqslant a$，

$$a \cup c = b \cup c,\ a \cap c = b \cap c，则有$$

$$a = a \cap (a \cup c) = a \cap (b \cup c) = b \cup (a \cap c) = b \cup (b \cap c) = b。$$必要性成立。

充分性。对任意 $a, b, c, b \leqslant a$，由模不等式 $b \cup (a \cap c) \leqslant (b \cup c) \cap a$，

令 $u = b \cup (a \cap c)$，$v = (b \cup c) \cap a$，

$$u \cup c = b \cup (a \cap c) \cup c = b \cup c,$$

$$v \cup c = ((b \cup c) \cap a) \cup c \leqslant (b \cup c) \cup c = b \cup c = u \cup c。$$

但 $u \leqslant v$，所以 $u \cup c \leqslant v \cup c$，则 $v \cup c = u \cup c$。

$$v \cap c = (b \cup c) \cap a \cap c = a \cap c,$$

$$u \cap c = (b \cup (a \cap c)) \cap c \geqslant (a \cap c) \cap c = a \cap c = v \cap c,$$

而 $u \leqslant v$，$u \cap c \leqslant v \cap c$，所以 $u \cap c = v \cap c$。

根据条件则 $u = v$，即 $b \cup (a \cap c) = (b \cup c) \cap a$。充分性成立。

定理 10.3.1 给出了模格的一个充要条件，对研究模格性质很有用处，但用于判断一个格是否为模格还不够直观。下面这个定理运用定理 10.3.1 的结论，其条件更为直观。

定理 10.3.2 设 S 是一个格，则 S 是模格当且仅当 S 没有与图 10.6(a)的格 $L1$ 同构的子格。

证明：必要性。知 S 是模格，假如 S 有与 $L1$ 同构之子格，由 10.3.1 已知 $L1$ 不是模格，则与 $L1$ 同构的 S 的子格也不是模格，因子格中 $\cap$ · $\cup$ 运算与 S 中相同，所以 S 也不是模格。

充分性。知 S 没有与 $L1$ 同构的子格，假如 S 不是模格，根据定理 10.3.1 可知存在 a，b，$c \in S$，$b \leqslant a$ · $a \cup c = b \cup c$，$a \cap c = b \cap c$，但 $a \neq b$。

我们说明 $A=\{a, b, c, a\cup c, a\cap c\}$ 即构成与 $L1$ 同构的 S 的子格，如图 10.7 所示：

首先易验证 A 关于 S 的运算$\cap$. $\cup$封闭，下面验证 A 中五个元素互不相同。

已知 $b\neq a$，再证 c 与 a 无关，否则 c 有可能：

(1) $c\geqslant a$，此时 $a\cap c=a\neq b=b\cap c$，矛盾。

(2) $c<a$，此时 $b\cap c=a\cap c=c$，得 $c\leqslant b$，

但若 $c\leqslant b$，则 $b\cup c=b\neq a=a\cup c$，矛盾。

因此 c 必与 a 无关，类似可证 c 与 b 无关。由 c 与 a、b 无关又可知 $a\cup c$ 大于 a，b，c，$a\cap c$ 小于 a，b，c，即集合 A 确实构成如图 10.7 所示之子格，从而 A 与 $L1$ 同构。与前提 S 没有与 $L1$ 同构子格矛盾，所以假设错误，S 必为模格。

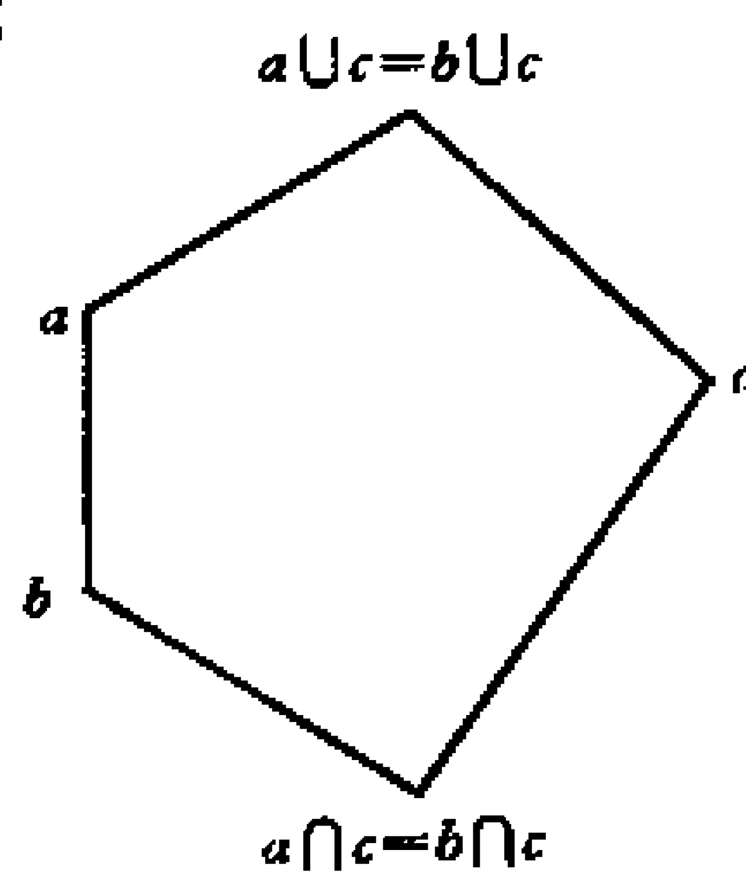


图 10.7

有了定理 10.3.2，在判定一个格是否为模格时，只要看它是否有 $L1$ 形式的子格，若有，则非模格，若无，则是模格，因而该定理在应用中较方便、直观。

比模格要求更强的是分配格。

定理 10.3.3 设 S 是一个格，以下三个命题等价：

(1) 对所有 $a, b, c\in S$，$a\cap(b\cup c)=(a\cap b)\cup(a\cap c)$。

(2) 对所有 $a, b, c\in S$，$a\cup(b\cap c)=(a\cup b)\cap(a\cup c)$。

(3) 对所有 $a, b, c\in S$，$(a\cap b)\cup(b\cap c)\cup(c\cap a)=(a\cup b)\cap(b\cup c)\cap(c\cup a)$。

证明：先证(1)=>(2)：

注意：不能应用格中的对偶原理，因为 (1) 不是对所有格都成立的命题。只有当一个命题 P 对所有格都成立时，才能应用对偶原理说明 P 的对偶命题对所有格也成立。

现已知 (1)，对所有 $a, b, c\in S$，

$$\begin{aligned}(a\cup b)\cap(a\cup c)&=((a\cup b)\cap a)\cup((a\cup b)\cap c)\\&=a\cup((a\cap c)\cup(b\cap c))\\&=a\cup(b\cap c)。\end{aligned}$$

再证 (2) => (1)：

此时可用对偶原理，(2)=>(1)与(1)=>(2)是对偶命题，(1)=>(2)对所有格都成立，则(2)=>(1)对所有格也成立。

再证(1)=>(3)： 首先(1)成立时(2)也成立。

对所有 $a,b,c\in S$，

$$\begin{aligned}(a\cap b)\cup(b\cap c)\cup(c\cap a)&=(b\cap(a\cup c))\cup(c\cap a)\\&=(b\cup(c\cap a))\cap((a\cup c)\cup(c\cap a))\\&=(b\cup c)\cap(b\cup a)\cap(a\cup c)。\end{aligned}$$

最后证 (3) => (1)：

首先证明 (3) 成立时模律成立，对任意 a，$b\in S$，$a\leqslant b$，

则 $$\begin{aligned}(a\cap b)\cup(b\cap c)\cup(c\cap a)&=a\cup(b\cap c)\cup(c\cap a)\\&=a\cup(b\cap c)。\end{aligned}$$

$$(a\cup b)\cap(b\cup c)\cap(c\cup a)=b\cap(b\cup c)\cap(c\cup a)$$

$=b\cap(c\cup a)$。

由(3)得　$a\cup(b\cap c)=b\cap(c\cup a)$，模律成立。

当（3）成立时以 a 并（3）中等式左右，得

$$a\cup(b\cap c)=a\cup((a\cup b)\cap(b\cup c)\cap(c\cup a))。$$

因为　$a\leqslant(a\cup b)\cap(a\cup c)$，所以可用模律于上等式右部，得

$$a\cup(b\cap c)=(a\cup b)\cap(c\cup a)\cap(a\cup b\cup c)=(a\cup b)\cap(a\cup c)。$$

（2）成立，则（1）成立。

上面定理证明中对偶原理的应用请大家注意。

定理 10.3.3 说明了分配律的几个形式是等价的，那么用任何形式都可给出分配格的定义。

定义 10.3.2　设（S、$\cup$、$\cap$）是一个格，若对任意的 a，b，$c\in S$，都有

$a\cap(b\cup c)=(a\cap b)\cup(a\cap c)$，则称 S 是分配格。

例 10.3.3　设 A 是一个集合，则($\rho(A)$，$\cup$，$\cap$)是分配格，因为集合 A 的各个子集之间的$\cap$，$\cup$运算满足分配律。

例 10.3.4　每个链都是分配格。

证明：设（S，$\leqslant$）是一个链，显然它是一个格。对任意 a，b，$c\in S$，它们的相互关系只有以下两种可能：

（1）$a\leqslant b$ 或 $a\leqslant c$，

（2）$b\leqslant a$ 且 $c\leqslant a$。

对于情况（1），由于 $a\leqslant b\cup c$，故 $a\cap(b\cup c)=a$，同时 $a\cap b\leqslant a$，$a\cap c\leqslant a$，而且这两个不等式中一定有一个使等式成立。因此$(a\cap b)\cup(a\cap c)=a$，亦即 $a\cap(b\cup c)=(a\cap b)\cup(a\cap c)$。

对于情况（2），一定有 $b\cup c\leqslant a$，因此 $a\cap(b\cup c)=b\cup c$，同时因为 $a\cap b=b$，$a\cap c=c$，故$(a\cap b)\cup(a\cap c)=b\cup c$。因此等式 $a\cap(b\cup c)=(a\cap b)\cup(a\cap c)$也成立，于是定理得证。

定理 10.3.4　分配格是模格。

在定理 10.3.3 的证明中，当证明（3）=>（1）时，实际已证明分配律包含模律，也即分配格是模格，这说明分配格的确是比模格条件强的一类格。

容易验证模格和分配格的对偶格也分别是模格和分配格，因此在模格和分配格中也有对偶原理，即若一个命题 P 对所有模格（或对所有分配格）都成立时，其对偶命题 P' 也对所有模格（或对所有分配格）成立。

定理 10.3.5　设<S，$\cup$，$\cap$>是一个格，则 S 是分配格的充要条件是对所有 a，b，$c\in S$，$a\cap(b\cup c)\leqslant(a\cap b)\cup c$。

证：必要性：　已知 S 是分配格，则 $a\cap(b\cup c)=(a\cap b)\cup(a\cap c)$，而$(a\cap c)\leqslant c$ 所以

$$a\cap(b\cup c)\leqslant(a\cap b)\cup c。$$

充分性：　由格的性质已知对所有 a，b，$c\in S$，

$(a\cap b)\cup c\leqslant(a\cup c)\cap(b\cup c)$，

只要证　$(a\cup c)\cap(b\cup c)\leqslant(a\cap b)\cup c$。

由条件知$(a\cup c)\cap(b\cup c)\leqslant((a\cup c)\cap b)\cup c\leqslant((a\cap b)\cup c)\cup c=(a\cap b)\cup c$，得证。

定理 10.3.6 设$<S, \cup, \cap>$是一个分配格，则对任意 a，b，$c \in S$，若 $a \cap b = a \cap c$，$a \cup b = a \cup c$，则 $b = c$。

证明：　由条件

$b = b \cap (a \cup b) = b \cap (a \cup c) = (b \cap a) \cup (b \cap c) = (a \cap c) \cup (b \cap c) = (a \cup b) \cap c = (a \cup c) \cap c = c$. 即 $b = c$。

定理 10.3.6 给出了 S 是分配格的一个必要条件。事实上，该条件是充要条件，但充分性较难证明，这在后面将会说明。

定理 10.3.6 的条件与定理 10.3.1 的条件相同，只少一个 $b \leqslant a$ 的要求，由此也可见分配格与模格相似，但分配格要求更强。

由定理 10.3.6 可判定某些格不是分配格。

例 10.3.5 图 10.6 中的格 $L1$，$L2$ 都不是分配格。

证明：取格 $L1$、$L2$ 中的 b，c，d，都有 $b \cup d = c \cup d = a$，$b \cap d = c \cap d = e$，但 $b \neq c$，所以，$L1$，$L2$ 都不是分配格。由定理 10.3.2 可知 $L1$ 可用来判断一个格是否为模格，同样 $L1$，$L2$ 也可以用来判断一个格是否为分配格。因此 $L1$，$L2$ 是两个很重要的格。

定理 10.3.7 （1）已知 S 是模格，S 不是分配格的充要条件是 S 包含与 $L2$ 同构的子格；（2）一个格 S 是分配格的充要条件是 S 不包含与 $L1$ 或 $L2$ 同构的子格。

定理中（1）与（2）论述的意思实际上相同，其中（1）的充分性和（2）的必要性的证明是显然的，但（1）的必要性和（2）的充分性证明较困难，有兴趣的读者也不妨一试。有了定理 10.3.7，对分配格的研究就会比较方便，例如定理 10.3.6 中的必要条件可证为充要条件。

定理 10.3.8 设$<S, \cup, \cap>$是一个格，如果对任意 a，b，$c \in S$，由 $a \cap b = a \cap c$，$a \cup b = a \cup c$，能得到 $a = b$，则 S 是分配格。

证明：假设 S 不是分配格，由定理 10.3.7 知 S 有与 $L1$ 或 $L2$ 同构的子格 A，不妨仍用图 10.6 中格 $L1$，$L2$ 的记号，取 b，c，d，都有 $b \cap d = c \cap d = e$，$b \cup d = c \cup d = a$，但 $b \neq c$ 与已知条件矛盾，因此 S 是分配格。

以下介绍有补格。

在偏序集中有极大元和极小元的概念，在格中也同样有这两个概念，而且容易证明，若一个格中存在有极大(小)元，则它是唯一的，称为最大(小)元。这样我们可以用 1 表示格中最大元，用 0 表示其最小元。

定义 10.3.3 设 S 是一个格，若 S 中存在 1 和 0 时，称 S 是有界格。

例如，设 A 一个集合，则$(\rho(A), \cup, \cap)$是有界格，其最大元 $1 = A$，最小元 $0 = \varnothing$。

定理 10.3.9 设 $(S, \leqslant)$ 是一个有界格，a 是 S 中的任意元，一定有

$$a \cup 1 = 1,\ a \cup 0 = a,$$
$$a \cap 1 = a,\ a \cap 0 = 0。$$

证明：因为 S 是有界格，所以有 1 和 0 存在，因为 1 是最大元，$a \leqslant 1$ 则 $a \cup 1 = 1$，$a \cap 1 = a$。同理因为 0 是最小元，$0 \leqslant a$，则 $a \cup 0 = a$，$a \cap 0 = 0$。

定义 10.3.4 设 $(S, \cup, \cap)$ 是一个有界格，对于 $a \in S$，若存在 $b \in S$，满足 $a \cup b = 1$，$a \cap b = 0$，则称 b 是 a 的补元，a 是 S 中的一个有补元。

显然，若b是a的补元，则a也是b的一个补元，不过补元不一定唯一。

例10.3.6 对图10.6中的格$L1$，$L2$，a即为最大元1，e即为最小元0，在$L1$中，b，c的补元都是d，d的补元就有b，c两个，在$L2$中，b，c，d中任意两个都互补，可见补元不一定唯一。

例10.3.7 设格$(S, \cup, \cap)$如图10.8所示，其中1的补元是0，0的补元是1，a和b没有补元。

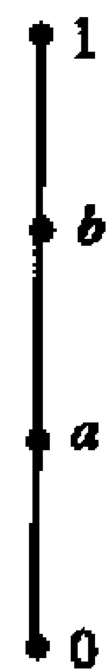


图 10.8

定义10.3.5 设$(S, \cup, \cap)$是有界格，若对任意$a \in S$，都有补元存在，则称S是有补格。

比如图10.6中两个格$L1$，$L2$都是有补格，而图10.8中格不是有补格。再如，设A是任一有限集，则$(\rho(A), \cup, \cap)$也是有补格，其中任意元B的补元是$A-B$。

在有补格S中元素a的补元并不一定唯一，但是如果S又是分配格的话，则补元一定是唯一的。对此我们有如下定理：

定理10.3.10 设S既是有补格，又是分配格，则S中的任一元素都有唯一的补元。

证明：设a是S中的一个元素，b、c都是a的补元，则

$$a \cup b = 1,\ a \cup c = 1,$$
$$a \cap b = 0,\ a \cap c = 0。$$

由定理10.3.6，有$b=c$。因此补元是唯一的。

这样我们可以得到有补分配格的概念。

定义10.3.6 如果格$(S, \cup, \cap)$既是分配格又是有补格，就称S是一个有补分配格。

例10.3.8 幂集格$(\rho(A), \cup, \cap)$是有补分配格。

有补分配格是一类很重要的代数系统，它就是下节要介绍的布尔代数。

10.4 布尔代数

定义10.4.1 一个有补分配格称为一个布尔代数。

很清楚，一个布尔代数中一定存在有最小元0，最大元1，而且对每个元素a，都有其唯一的补元a'，满足

$$a \cup a' = 1,\ a \cap a' = 0。$$

一般我们用$(B, \cup, \cap, ', 0, 1)$表示一个布尔代数，其中$(B, \cup, \cap)$是一个格，$(B, \leqslant)$是相应的偏序集。0和1是格B中的最小元和最大元，由于有补格B中的任一元a都有唯一的补元$a' \in B$，所以可以在格B中规定一个一元的求补运算“$'$”。

例10.4.1 设$A=\{a\}$，则$\rho(A)=\{\varnothing, A\}$，幂集格$(\rho(A), \cup, \cap, ', 0, 1)$是一个布尔代数，其中$0=\varnothing$，$1=A$，其运算表如下

$\cup$	O	A
O	O	A
A	A	A

$\cap$	O	A
O	O	O
A	O	A

·	$'$
O	A
A	O

在本章的讨论中，我们不断对格增加了一些附加条件，得到一些特殊的代数系统。图 10.9 表示出这些代数系统从简单到特殊的关系。在这些代数系统中，又往往列举了幂集格的例子。它说明幂集格都满足这些附加的条件，事实上，如果某个代数系统能够与一个幂集格同构，那么这样的代数系统就是布尔代数。更重要的是，任何有限布尔代数都与某幂集格同构。这也是本节中我们将要重点讨论的内容。

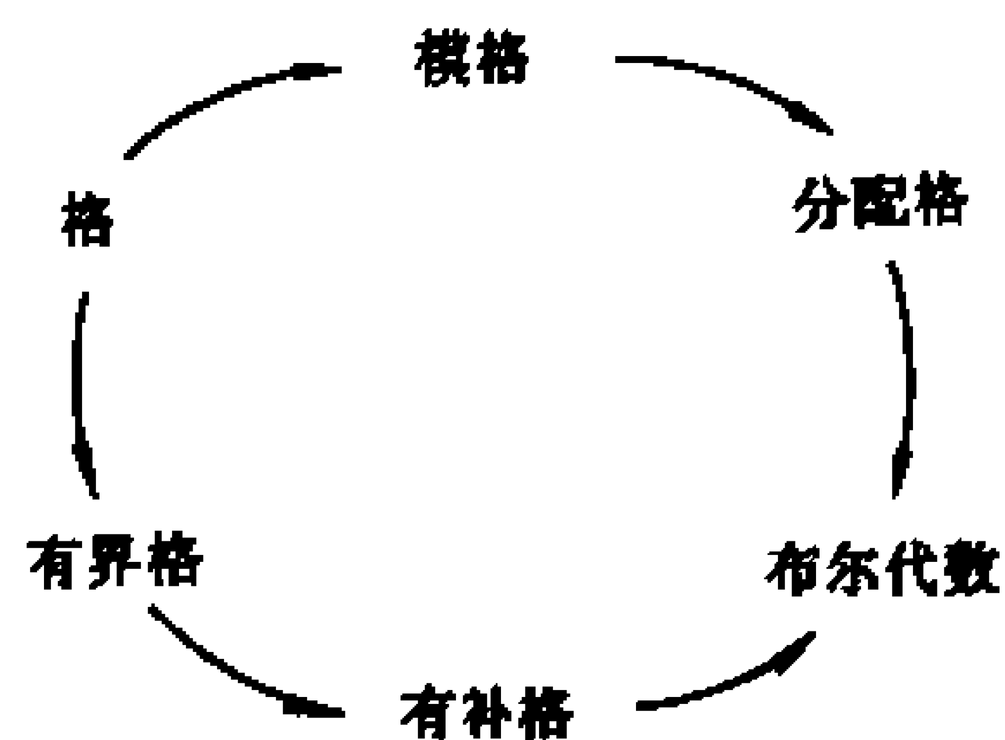


图 10.9

例 10.4.2 令 A 表示含有 n 个命题变元的命题公式的集合，则代数系统 $(A, \vee, \wedge, \neg, F, T)$ 是一个布尔代数，称为命题代数，其中 $\vee$，$\wedge$ 分别是析取和合取运算，$\neg$ 是否定运算，F 和 T 分别是永假式和永真式。

例 10.4.3 一个开关代数 $(A_n, +, \cdot, -, 0_n, 1_n)$ 也是一个布尔代数，A_n 是 n 元组的集合，即 A_n 的任一元素 $a=\langle a_1, a_2, \cdots, a_n\rangle$，其中 $a_i=0$ 或 1，$i=1, 2, \cdots, n$。对 A_n 中的元素 $a=\langle a_1, a_2, \cdots, a_n\rangle$，$b=\langle b_1, b_2, \cdots, b_n\rangle$，定义

$$a+b=\langle a_1 \vee b_1, a_2 \vee b_2, \cdots, a_n \vee b_n\rangle。$$

$$a \cdot b=\langle a_1 \wedge b_1, a_2 \wedge b_2, \cdots, a_n \wedge b_n\rangle。$$

$$\bar{a}=\langle \bar{a}_1, \bar{a}_2, \cdots, \bar{a}_n\rangle。$$

这里 $\vee$，$\wedge$，是一般的逻辑运算，因此 A_n 中的最小元是 $0_n=\langle 0, 0, \cdots, 0\rangle$，最大元是 $1_n=\langle 1, 1, \cdots, 1\rangle$。$A_n$ 是一个布尔代数，通常称为开关代数。

这些例子说明，命题代数、开关代数以及集合代数都是布尔代数的特例。

因为布尔代数是一个有补分配格，所以它具有下述性质：

设 $a, b, c \in B$。

1. 因为 $(B, \cup, \cap)$ 是格，所以运算 $\cup$ 和 $\cap$ 满足：

(1.1) $a \cup a=a, a \cap a=a$。

(1.2) $a \cup b=b \cup a, a \cap b=b \cap a$。

(1.3) $(a \cup b) \cup c=a \cup (b \cup c)$。

$(a \cap b) \cap c=a \cap (b \cap c)$。

(1.4) $a \cap (b \cup a)=a$。

$a \cup (b \cap a)=a$。

2. 因为 $(B, \cup, \cap)$ 是分配格，所以有恒等式：

(2.1) $a \cap (b \cup c)=(a \cap b) \cup (a \cap c)$。

$a \cup (b \cap c)=(a \cup b) \cap (a \cup c)$。

3. 由于 $(B, \cup, \cap, 0, 1)$ 是有界格，所以有下述关系：

(3.1) $0 \leqslant a \leqslant 1$。

(3.2) $a \cap 0=0$，$a \cup 1=1$。

(3.3) $a \cup 0=a$，$a \cap 1=a$。

4. 由于 $(B, \cup, \cap, ', 0, 1)$ 是有补格，设 a' 是 a 的补元，则它满足下列恒等式：

(4.1) $a \cap a'=0$，$a \cup a'=1$。

(4.2) $0'=1$，$1'=0$。

(4.3) $(a')'=a$。

在布尔代数中也有对偶原理。因为将一个布尔代数中$\cup$，$\cap$运算互换，0，1互换就可得到相应的对偶布尔代数，且其中互补元素不变。所以若一个命题P对所有布尔代数都成立，则将P中$\cup$与$\cap$互换，$\leqslant$与$\geqslant$互换，0与1互换，得到对偶命题P'，P'对所有布尔代数也成立。上面从（1.1）到（4.3）各性质中的两个等式实际上都是互为对偶的命题。

在布尔代数中，求补运算$'$与运算$\cup$和$\cap$之间有密切的联系。

定理 10.4.1 设a，b是布尔代数$(B,\cup,\cap,',0,1)$中的任意两个元素，恒有

$$(a\cap b)'=a'\cup b',\ (a\cup b)'=a'\cap b'。$$

证明：设a'，b'分别是B中a和b的补元，则

$$\begin{aligned}(a\cap b)\cap(a'\cup b')&=((a\cap b)\cap a')\cup((a\cap b)\cap b')\\&=((a\cap a')\cap b)\cup(a\cap(b\cap b'))\\&=0\cup 0=0。\end{aligned}$$

$$\begin{aligned}(a\cap b)\cup(a'\cup b')&=(a\cup(a'\cup b'))\cap(b\cup(a'\cup b'))\\&=((a\cup a')\cup b')\cap((b\cup b')\cup a')\\&=1\cap 1=1\end{aligned}$$

因此$(a'\cup b')$是$(a\cap b)$的补元，即$(a\cap b)'=a'\cup b'$。根据布尔代数中的对偶原理，$(a\cup b)'=a'\cap b'$。

该式就是著名的摩根定律。依据数学归纳原理，可以把结合律、分配律以及摩根律加以推广，从而得到

(5.1) $(\bigcup_{i=1}^{p}a_i)\cup(\bigcup_{j=p+1}^{t}a_j)=\bigcup_{l=1}^{t}a_l$，

式中a_j出现的次序是任意的。

(5.2) $(\bigcap_{S}a_i)\cup(\bigcap_{T}b_j)=\bigcap_{S\times T}(a_i\cup b_j)$，

$(\bigcup_{S}a_i)\cap(\bigcup_{T}b_j)=\bigcup_{S\times T}(a_i\cap b_j)$。

(5.3) $(\bigcap_{S}a_i)'=\bigcup_{S}a_i'$，$(\bigcup_{S}a_i)'=\bigcap_{S}a_i'$。

式中S的元素是i，$i=1,2,\cdots,n$；T的元素是j，$j=1,2,\cdots,m$。

布尔代数与群、环和域一样，有其子代数的概念。

定义 10.4.2 设$(S,\cup,\cap,',0,1)$是一个布尔代数，且$T\subseteq S$，若$0,1\in T$且对任意$a,b\in T$，$\cup$、$\cap$、$'$运算都是封闭的，则称T是S的一个子布尔代数。

例 10.4.4 设$A=\{a,b,c\}$，则$T=\{\varnothing,\{a,b\},\{c\},A\}$是$\rho(A)$的一个子布尔代数，如图10.10所示。

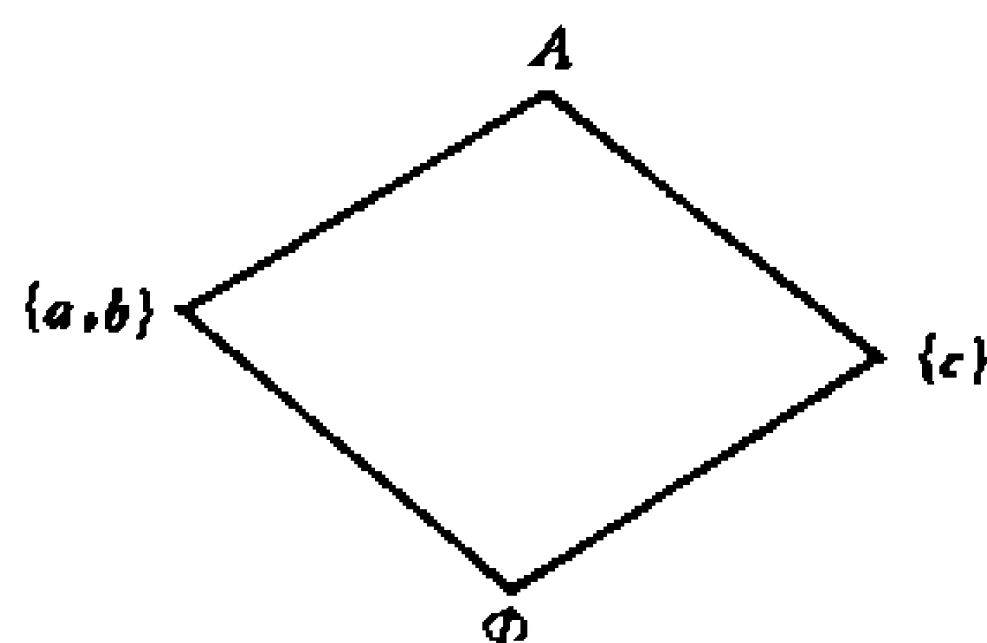


图 10.10

应该注意，虽然有的$T\subseteq S$能够构成一个布尔代数，却不一定是S的子布尔代数，这是因为对S中的运算来说，T可以不是封闭的。读者可以试举这样的例子。

至此，我们可以得到统一的关于子代数的定义。

定义 10.4.3 设 A 是具有一组运算的集合 Ω 的代数系统，B 是 A 的非空子集。如果 B 关于 Ω 中的每一运算都是封闭的，则称 B 是 A 的一个子代数。

定义 10.4.4 设 $(A, \cup, \cap, ',)$ 和 $(B, \cup, \cap, ',)$ 是两个布尔代数，如果存在着 A 到 B 的映射 f，对于任意的 a，$b\in A$，都有

$$f(a\cup b)=f(a)\cup f(b)。$$
$$f(a\cap b)=f(a)\cap f(b)。$$
$$f(a')=(f(a))'。$$

则称 f 是 A 到 B 的一个布尔同态。如果 f 分别是单射、满射和双射，则分别称为单一同态、满同态和同构。

由同态的定义可知 $f(0)=0, f(1)=1$，因为 $f(0)=f(a\cap a')=f(a)\cap f(a')=f(a)\cap (f(a))'=0, f(1)=f(a\cup a')=f(a)\cup f(a')=f(a)\cup (f(a))'=1$。

设 A 是具有 n 个元的集合，我们知道$(\rho(A), \cup, \cap, ', 0, 1)$是含有 2^n 个元的布尔代数。如果一个布尔代数的元素数目有限，我们称之为有限布尔代数。可以证明，任何有限布尔代数一定与某个$(\rho(A), \cup, \cap, ', 0, 1)$同构。该结论称之为 Stone 表示定理，为证明这个定理需要先介绍一些必要的概念与预备定理。

定义 10.4.5 设 $(B, \leqslant)$ 是一个格，若存在 $a\in b$，$a\neq 0$，满足对所有 B 中的小于等于 a 的元素 x，一定有 $x=0$ 或 $x=a$，称 a 是 B 中的一个原子或极小项。

比如在图 10.11 的格中，d，b，f 都是原子，它说明格中的原子并不唯一。很明显，如果 a，b 都是格 B 中的原子，且 $a\neq b$，那么一定有 $a\cap b=0$。

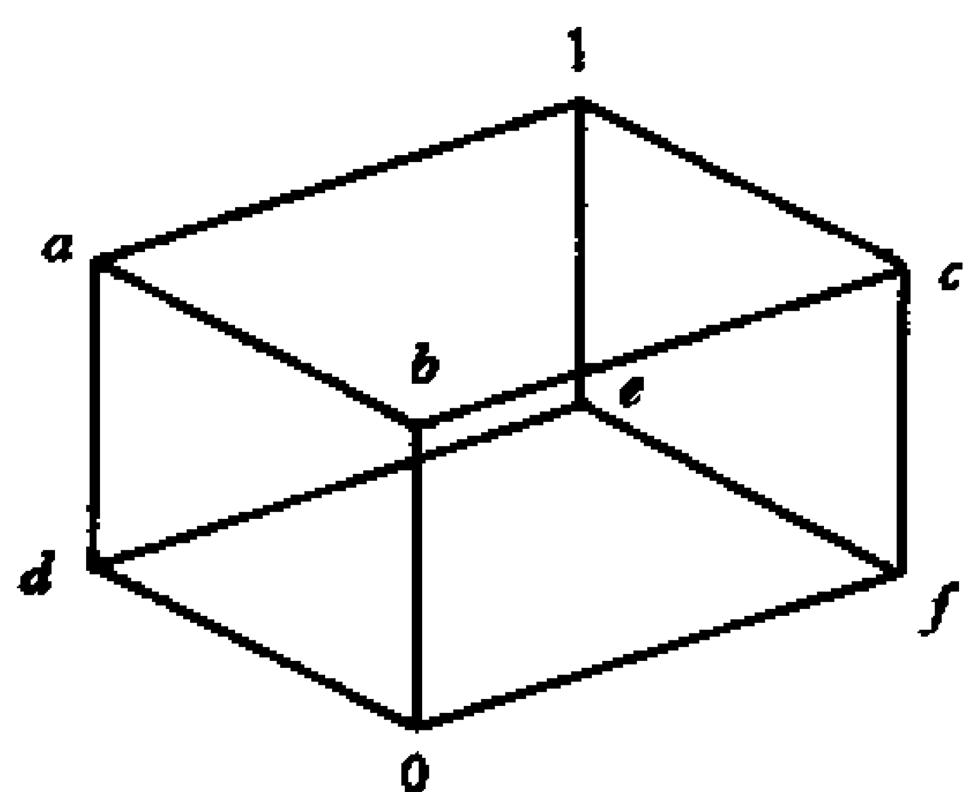


图 10.11

定理 10.4.2 设 $(B, \leqslant)$ 是具有最小元 0 的有限格，则对于任何一个非 0 元 a，至少存在一个原子 b，使 $b\leqslant a$。

证明：若 a 本身就是原子，则 $a\leqslant a$ 成立。若 a 不是原子，则一定有元素 b_1，满足 $0<b_1<a$，若 b_1 是原子，则 b_1 即为所求，否则一定存在一条链，使

$$0<b_i<\cdots<b_2<b_1<a,$$

且不存有其它元素小于 b_i，则 b_i 就是所求的一个原子。

当然 b_i 并不一定唯一，比如图 10.11 中，$0<b<c$，$0<f<c$，所以对元素 c 而言，可以有两个原子 b 和 f 都满足定理要求。

定理 10.4.3 在一个布尔格中，$b\cap c'=0$ 的充要条件是 $b\leqslant c$。

该定理的证明请读者自行完成。

定理 10.4.4 在布尔格 $(B, \leqslant)$ 中，设 a 是任一原子，b 是 B 中任意元素，那么 $a\leqslant b$ 和 $a\leqslant b'$ 中有且仅有一式成立。

证明：若两式能同时成立，则 $a\leqslant b\cap b'=0$，产生矛盾。因为 a 是原子，所以只能有两种情况，即 $a\cap b=0$ 或 $a\cap b=a$，若 $a\cap b=a$，则有 $a\leqslant b$；若 $a\cap b=0$，则 $a\cap (b')'=0$，由定理 10.4.3，即 $a\leqslant b'$。

定理 10.4.5 设 $(B, \cup, \cap, ', 0, 1)$ 是一个有限布尔代数，设 b 是其中的任意非 0

元，a_1，a_2，…，a_l 是满足 $a_i \leqslant b$ 的所有原子，则

$$b=a_1 \cup a_2 \cup \cdots \cup a_l。$$

证明：设 $x=a_1 \cup a_2 \cup \cdots \cup a_l$，因为 $a_i \leqslant b$，所以 $x \leqslant b$。以下再证 $b \leqslant x$，由定理 10.4.3，它等价于证明 $b \cap x'=0$。为此假定 $b \cap x' \neq 0$，由定理 10.4.2，应存在一原子 c，满足 $c \leqslant b \cap x'$。由于 $b \cap x' \leqslant x'$ 和 $b \cap x' \leqslant b$，故有 $c \leqslant x'$ 和 $c \leqslant b$，因为 c 是原子且满足 $c \leqslant b$，故 $c=a_j$ 即 c 就是满足 $a_j \leqslant b$ 中的某一个原子 a_j，故 $c \leqslant x$。这样 $c \leqslant x$ 和 $c \leqslant x'$ 同时成立，与定理 10.4.4 矛盾。
故 $b \cap x'=0$，定理得证。

定理 10.4.6 设 b 是有限布尔代数 $(B, \cup, \cap, ', 0, 1)$ 中的一个非 0 元，则不考虑顺序和无重复时，b 可以唯一地表示成

$$b=a_1 \cup a_2 \cup \cdots a_l。$$

其中 a_i（$i=1, 2, \cdots, l$）是 B 中所有满足 $a_i \leqslant b$ 的原子。

证明：设 b 有另一种表示形式

$$b=a_{j1} \cup a_{j2} \cup \cdots \cup a_{jk}。$$

其中 a_{ji}（$i=1, 2, \cdots, k$）也是 B 中的原子，不妨设 $k \leqslant l$，则存在一个原子 a_i 在第一种表示中出现但未在第二种表现中出现，因此

$$a_i \cap (a_{j1} \cup a_{j2} \cup \cdots \cup a_{jk})=a_i \cap (a_1 \cup a_2 \cup \cdots \cup a_l),$$

即

$$(a_i \cap a_{j1}) \cup (a_i \cap a_{j2}) \cup \cdots \cup (a_i \cap a_{jk})=a_i \cap b。$$

而因为 a_i 与 a_{jk}是不相同的原子，故 $a_i \cap a_{js}=0$，$s=1, 2, \cdots, k$，于是有 $0=a_i$。
产生矛盾。故 b 的表示方式唯一。

上面我们讨论了原子的某些重要性质，它揭示了一个布尔代数 $(B, \cup, \cap, ', 0, 1)$ 和其原子集合 $S=\{a_1, a_2, \cdots, a_n\}$ 之间的关系，即除了最小元 0 以外，B 中的各个元素都可以唯一地用其原子的“$\cup$”运算表示，或者说可以用 S 的某个子集与之对应。事实上，S 中每一个这样的“$\cup$”运算，都表示了 B 中的一个对应元素，也就是说在 S 的子集与 B 的元素之间，存在着一个一一对应关系，这种关系能够保持$\cup$，$\cap$和$'$运算，即布尔代数 $(B, \cup, \cap, ', 0, 1)$ 与集合代数$(\rho(S), \cup, \cap, -, \varnothing, S)$同构。

定理 10.4.7 （Stone 表示定理）设 $(B, \vee, \wedge, ', 0, 1)$ 是由有限布尔格 $\langle B, \leqslant\rangle$ 所诱导的布尔代数，S 是 $\langle B, \leqslant\rangle$ 中所有原子的集合，则 $(B, \vee, \wedge, ', 0, 1)$ 与 $(\rho(S), \cup, \cap, -, \varnothing, S)$ 同构。

证明：由定理 10.4.6，知 B 中任一非 0 元素 b，都有唯一的原子表示形式

$$b=a_1 \vee a_2 \vee \cdots \vee a_l。$$

令 $S_b=\{a_1, a_2, \cdots, a_l\}$，则 $S_b \in \rho(S)$，因此可作映射 f

令 $f(0)=\varnothing$

对任一非 0 元 $b \in B$，令 $f(b)=S_b$,因此 f 是 B 到 $\rho(S)$的一个映射。

如果对 $S_b \in \rho(S)$，存在 a，$b \in B$，满足 $f(a)=f(b)=S_b$，则由定理 10.4.5，$a=a_1 \vee a_2 \vee \cdots \vee a_l=b$，即 $a=b$，故 f 是单射。

对于任意的 $S_b \in \rho(S)$，$S_b=\{a_1, a_2, \cdots, a_l\}$，则由运算$\cup$的封闭性，$a_1 \vee a_2 \vee \cdots \vee a_l$

$\in B$，因此 f 是满射。

因此 f 是 B 到 $\rho(S)$ 的一个双射。下面证明 f 是同构。这就要求对任意 a，$b\in B$，

1. $f(a\vee b)=f(a)\cup f(b)$。

2. $f(a\wedge b)=f(a)\cap f(b)$。

3. $f(a')=f(a)$。

设 $f(a)=S_1=\{a_1,a_2,\cdots,a_n\}$，

$f(b)=S_2=\{b_1,b_2,\cdots,b_m\}$。

因 f 是满射，所以存在 $x\in B$，$f(x)=s_1\cup s_2=f(a)\cup f(b)$，即 $s_1\cup s_2$ 包含了所有小于等于 x 的原子，则由定理 10.4.5，$x=a_1\vee a_2\vee\cdots\vee a_n\vee b_1\vee b_2\vee\cdots\vee b_m=a\vee b$，即 $f(a\vee b)=f(a)\cup f(b)$

根据分配律可以有

$$a\wedge b=(a_1\vee a_2\vee\cdots\vee a_n)\wedge(b_1\vee b_2\vee\cdots\vee b_m)$$
$$=\bigvee_{i=1}^{n}\{\bigvee_{j=1}^{m}(a_i\wedge b_j)\}。$$

由于 a_i，b_j 都是原子，因此

$$a_i\wedge b_j=\begin{cases}a_i(=b_j), & a_i=b_j。\\ 0 & a_i\neq b_j。\end{cases}$$

故 $(a\wedge b)$ 是全部 $a_i=b_j$ 的元素之间进行 $\vee$ 运算的结果，所以

$$f(a\wedge b)=S_1\cap S_2=f(a)\cap f(b)。$$

最后我们再证明 $f(a')=f(a)$。由于 $a\vee a'=1$，$a\wedge a'=0$，故 $f(a\vee a')=S$，$f(a\wedge a')=\varnothing$，由上已知 f 保持交，并运算，则有 $f(a)\cup f(a')=S$，$f(a)\cap f(a')=\varphi$，即

$$f(a')=f(a)。$$

综上说明 f 保持运算。定理得证。

由 Stone 定理可以得到以下推论：

推论 1：有限布尔格的元素数目是 2^n 个，其中 n 是该布尔格中所有原子的个数。

推论 2：任何两个具有 2^n 个元素的布尔代数都是同构的。

10.5 布尔表达式

设 $\{x_1, x_2, \cdots, x_n\}$ 是 n 个变元的集合，由这些变元与运算 $\cup$，$\cap$ 和 $'$ 可以构成形形色色的字符串，其中的一些称之为布尔表达式。

定义 10.5.1 设 x_1，x_2，$\cdots$，x_n 是 n 个变元，$(B, \cup, \cap',)$ 是一个布尔代数，则

1. B 中任何元素是一个布尔表达式。

2. 任何变元 x_i 是一个布尔表达式。

3. 如果 a_1 和 a_2 是布尔表达式，则 $(a_1)'$，$(a_1\cup a_2)$ 和 $(a_1\cap a_2)$ 也是布尔表达式。

4. 只有通过有限次使用规则 1，2，3 构造的符号串才是布尔表达式。

在一般不会造成误解的情况下，省略一些括号也允许。

例 10.5.1 $(\{0,1,2,3\},\cup,\cap,')$ 是一个布尔代数，如图 10.12 所示。则 2，$(1\cup x_2)$，$(x_1\cap x_3)\cup 0$，$(1'\cap(2\cup x_1))\cup(1\cap x_2')$ 等都是布尔表达式。

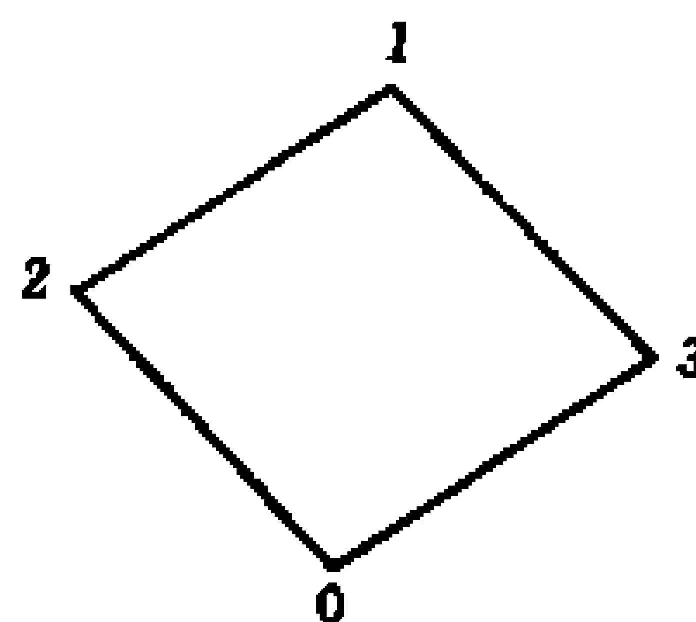


图 10.12

我们用 $E(x_1, x_2, \cdots, x_n)$ 表示一个可含有 n 个变元的布尔表达式，应该注意，n 元布尔表达式可以包括 n 个变元，也可以不包含这全部 n 个变元。

定义 10.5.2 设 $(B,\cup,\cap,')$ 是一个布尔代数，若布尔表达式 $E(x_1, x_2, \cdots, x_n)$ 中的 x_i $(i=1, 2, \cdots, n)$ 用 B 中某一确定元素来赋值，就得到了该布尔表达式 $E(x_1, x_2, \cdots, x_n)$ 的值。

比如上例中，设布尔表达式是

$$E(x_1,x_2,x_3)=(3\cup(x_1\cap x_3))\cap(x_1'\cup x_2)。$$

设 $x_1=2, x_2=0, x_3=1$，则有

$$E(2,0,1)=(3\cup(2\cap 1))\cap(2'\cup 0)=(3\cup 2)\cap(3\cup 0)=1\cap 3=3。$$

这就是该布尔表达式的值。

定义 10.5.3 设 $E_1(x_1, x_2, \cdots, x_n)$ 和 $E_2(x_1, x_2, \cdots, x_n)$ 是两个布尔表达式，若对 x_i $(i=1, 2, \cdots, n)$ 任意进行赋值：$x_i=x_i^0$，这两表达式的值恒定相等，即

$$E_1(x_1^0, x_2^0, \cdots, x_n^0)=E_2(x_1^0, x_2^0, \cdots, x_n^0)。$$

则称这两个布尔表达式是等价的(或相等的)。

当然，我们可以用定义的方法来验证两个布尔表达式的相等。另外我们也可以直接利用布尔代数的恒等式，对其中一个表达式经过有限次恒等变换后，能够得到另一个布尔表达式，那么它们也就是相等的。

布尔代数 $(B,\cup,\cap,')$ 上的任一个布尔表达式 $E(x_1, x_2, \cdots, x_n)$ 的值都是唯一确定的，显然，由于 $(B,\cup,\cap,')$ 是有补分配格，所以布尔代数运算的结果最终一定是 B 中的某个元素，即 $E(x_1^0, x_2^0, \cdots, x_n^0)\in B$。因此可以说布尔表达式确定了 B^n 到 B 的一个函数。

如果一个 B^n 到 B 的函数能够用 $(B,\cup,\cap,')$ 上的 n 元布尔表达式来表示，就称它是一个布尔函数。比如图 10.13 给出了 $\{0, 1\}^3$ 到 $\{0, 1\}$ 的一个函数 f。

	f
⟨000⟩	0
⟨001⟩	1
⟨010⟩	0
⟨011⟩	1
⟨100⟩	0
⟨101⟩	0
⟨110⟩	1
⟨111⟩	0

图 10.13

下面布尔表达式对 x_1，x_2，x_3 任意赋值得到结果都与 f 相同

$$(x'_1\cap x'_2\cap x_3)\cup(x'_1\cap x_2\cap x_3)\cup(x_1\cap x_2\cap x'_3)。$$

因此函数 f 是布尔函数。

定理 10.5.1 对二元布尔代数 $(\{0,1\},\cup,\cap,')$ 来说，任何一个从 $\{0, 1\}^n$ 到 $\{0, 1\}$ 的函数都是布尔函数。

证明：对含有 n 个变元的布尔表达式来说，我们称表达式 $x_1^0\cap x_2^0\cap\cdots\cap x_n^0$ 为小项，其中 x_i^0 是 x_i 或 x'_i 的任一个。如果一个布尔表达式能表示成小项之间的 $\cup$ 运算，则称之是析取范式。因此，对 $\{0, 1\}^n$ 到 $\{0, 1\}$ 的任一函数，对使其函数值为 1 的那些 n 元组分

别构造小项 $x_1^0 \cap x_2^0 \cap \cdots \cap x_n^0$，其中

$$x_i^0 = \begin{cases} x_i, \text{若该 } n \text{ 元组中第 } i \text{ 个分量为 } 1。\\ x_i', \text{若该 } n \text{ 元组中第 } i \text{ 个分量为 } 0。\end{cases}$$

这样，由全部这些小项进行$\cup$运算，就构成了析取范式。它就是一个布尔表达式，而且易验证它与原函数相对应，因此定理得证。

由函数值为 1 的小项可以构成析取范式，同样，根据函数值为 0，也可以构造大项。最后由合取范式来表示相应的布尔函数，比如上表中，它的合取范式是

$(x_1 \cup x_2 \cup x_3) \cap (x_1 \cup x'_2 \cup x_3) \cap (x'_1 \cup x_2 \cup x_3) \cap (x'_1 \cup x_2 \cup x'_3) \cap (x'_1 \cup x'_2 \cup x'_3)$。

因为从 $\{0, 1\}^n$ 到 $\{0, 1\}$ 的任何函数，它的函数值只可能是 1 或 0。因此析取范式和合取范式总是能够得到的。

习 题 十

1. 设 $A = \{\alpha, \beta, \gamma\}$，求格 $\langle 2^A, \subseteq \rangle$ 的图形。

2. 证明定理 10.1.4 中，$(a \cup b)$ 是 $\{a, b\}$ 的最小上界。

3. 证明定理 10.1.6。

4. 在格中，若 $a \leqslant b \leqslant c$，证明：

(1) $a \cup b = b \cap c$。

(2) $(a \cap b) \cup (b \cap c) = b = (a \cup b) \cap (a \cup c)$。

5. 证明定理 10.1.9。

6. 设 S_n 是 n 的所有因子的集合，令 $n = 24$，按例 10.1.4 所定义的偏序关系，求格 $(S_n, \cup, \cap)$ 的偏序图，并求它的全部子格。

7. 设 Z_+ 是例 10.2.1 中的格，试判断

(a) $\{1, 2, 3, 9, 24, 72\}$，

(b) $\{1, 2, 3, 12, 18\}$，

(c) $\{3, 3^2, 3^3, \cdots\}$，

中哪个是 Z_+ 的子格？

8. A、B 是两个集合，f 是 A 到 B 的映射，定义另一从 $\rho(A)$ 到 $\rho(B)$ 的映射 f'，对所有 $X \in \rho(A)$，

$f'(X) = \{f(x) \mid x \in X\} \in \rho(B)$。证明：

(1) 令 $S = \{f'(X) \mid X \in \rho(A)\}$，则 $\langle S, \subseteq \rangle$ 是 $\langle \rho(B) \subseteq \rangle$ 的子格。

(2) f' 是保并同态，但不一定是保交同态。

(3) 当且仅当 f 是单射时 f' 是保交同态，从而 f' 是格同态，且 f' 是单同态。

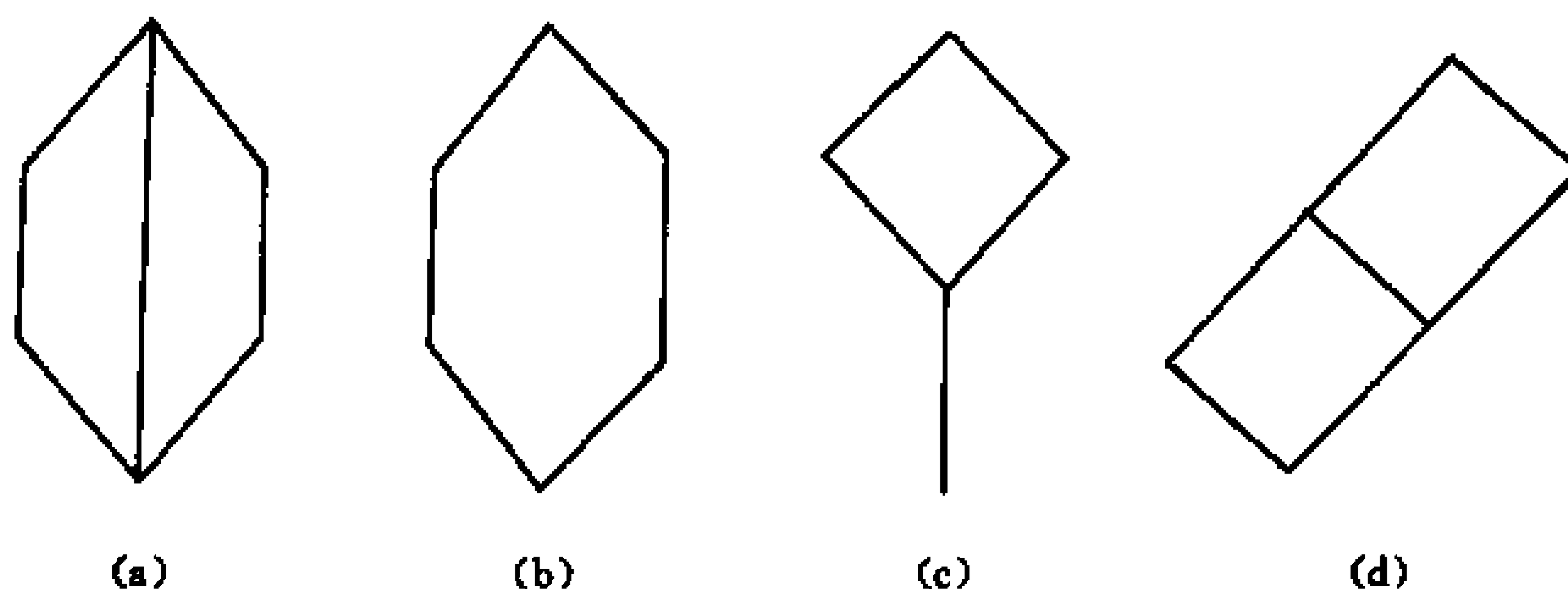
9. 证明定理 10.2.3 中的结论：保序同构等价于保并同构。

10. 设 f 是 S_1 到 S_2 的同态，g 是格 S_2 到 S_3 的同态，设 $g \cdot f$ 是 S_1 到 S_3 的映射，即对任意 $a \in S_1$，都有 $g \cdot f(a) \in S_3$，证明

(1) $g \cdot f$ 是 S_1 到 S_3 的同态。

(2) 若 g，f 都是同构，则 $g \cdot f$ 也是同构。

11. 题图 10.11 中，哪些是分配格，哪些是有补格？



题图　10.11

12. 举两个仅含 6 个元素的格，一个是分配格，另一个不是分配格的例子，并判断是不是模格和有补格。

13. 证明：若 $(S, \cup, \cap)$ 是分配格，则对任意 $a_i, b_j \in S$，$i=1, 2, \cdots, n$，$j=1, 2, \cdots, m$，有

$$(\bigcap_{i=1}^{n} a_i) \cup (\bigcap_{j=1}^{m} b_j) = \bigcap_{i=1}^{n} (\bigcap_{j=1}^{m} (a_i \cup b_j))。$$

$$(\bigcup_{i=1}^{n} a_i) \cap (\bigcup_{j=1}^{m} b_j) = \bigcup_{i=1}^{n} (\bigcup_{j=1}^{m} (a_i \cap b_j))。$$

14. 试证 3 个元素的链不是有补格。

15. 证明定理 10.3.7 。

16. 证明在有补分配格 $(S, \cup, \cap)$ 中，对任意 $a, b \in S$，有

(1) $b' \leqslant a' <=> a' \cup b = 1$。

(2) $a \leqslant b <=> a \cap b' = 0 <=> a' \cup b = 1$。

17. 设 $(B, \cup, \cap',)$ 是一个布尔代数，对于 $a, b \in B$，证明 $a \leqslant b$ 的充要条件是 $b' \leqslant a'$。

18. 证明下列布尔恒等式：

(1) $a \cup (a' \cap b) = a \cup b$。

(2) $a \cap (a' \cup b) = a \cap b$。

(3) $(a \cap b) \cup (a \cap b') = a$。

(4) $(a \cup b') \cap (b \cup c') \cap (c \cup a') = (a' \cup b) \cap (b' \cup c) \cap (c' \cup a)$。

19. 找出 8 元布尔代数的所有子代数。

20. 设 B 是元素数目大于 2 的布尔代数，任取 $a \in B$，$a \neq 0$，$a \neq 1$，证明 $T = \{0, a, a', 1\}$ 是 B 的一个子代数。

21. 给定从一个布尔代数到另一布尔代数的映射 f，试证明，如果 f 对 $\cup$ 和 $'$ 保持运算，则 f 是一个布尔同态。

22. 设 $(B, \cup, \cap',)$ 是一个布尔代数，若在 B 上定义二元运算 $\cdot$ 如下：

$$a \cdot b = (a \cap b') \cup (a' \cap b)。$$

证明 $(B, \cdot)$ 是一个交换群。

23. 证明定理 10.4.3。

24. 设 $E(x_1, x_2, x_3, x_4)=(x_1\cap x'_3)\cup(x_1\cap x_2\cap x'_4)\cup(x'_2\cap x_3\cap x_4)$是布尔代数$(\{0,1\},\cup,\cap,')$上的一个布尔表达式试写出它的析取范式与合取范式。

25. 对题图 10.25 中的函数 f，试用析取范式与合取范式表示之。

	f
⟨000⟩	0
⟨001⟩	1
⟨010⟩	1
⟨011⟩	0
⟨100⟩	1
⟨101⟩	0
⟨110⟩	1
⟨111⟩	0

题图 10.25

